ESET FILE SECURITY

POUR MICROSOFT WINDOWS SERVER

Manuel d'installation et guide de l'utilisateur

Microsoft® Windows® Server 2000 / 2003 / 2008 / 2008 R2 / 2012 / 2012 R2

Cliquez ici pour télécharger la dernière version de ce document.



ESET FILE SECURITY

Copyright © 2013 par ESET, spol. s r.o.
ESET File Security a été développé par ESET, spol. s r.o.

Pour plus d'informations, visitez www.eset.com.
Tous droits réservés. Aucune partie de cette documentation ne peut être reproduite, stockée dans un système d'archivage ou transmise sous quelque forme ou par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement, numérisation ou autre sans l'autorisation écrite de l'auteur.
ESET, spol. s r.o. se réserve le droit de modifier les applications décrites sans préavis.

Service client : www.eset.com/support

RÉV. 11/11/2013

Table des

1. Introduction

ESET File Security est une solution intégrée spécialement conçue pour l'environnement Microsoft Windows Server. ESET File Security offre une protection très efficace contre les différents types d'attaques par logiciels malveillants et fournit deux types de protection : Antivirus et antispyware.

Voici quelques-unes des principales fonctionnalités d'ESET File Security :

- Exclusions automatiques - détection et exclusion automatiques des fichiers essentiels du serveur afin de garantir un fonctionnement sans problème.
- eShell (ESET Shell) - nouvelle interface à ligne de commande qui offre aux utilisateurs chevronnés et aux administrateurs des options plus complètes pour gérer les produits ESET.
- SelfDefense - technologie permettant de protéger les solutions de sécurité ESET de toute modification ou désactivation.
- Dépannage efficace - intègre des outils avancés de résolution des différents problèmes : ESET SysInspector pour les diagnostics système et ESET SysRescue pour la création d'un CD de dépannage amorçable.

ESET File Security prend en charge Microsoft Windows Server versions autonomes 2000, 2003 et 2008, ainsi que Microsoft Exchange Server dans un environnement à cluster. Vous pouvez gérer ESET File Security à distance dans des réseaux de grande taille grâce à ESET Remote Administrator.

1.1 Configuration système

Systèmes d'exploitation pris en charge :

- Microsoft Windows 2000 Server
- Microsoft Windows Server 2003 (x86 et x64)
- Microsoft Windows Server 2008 (x86 et x64)
- Microsoft Windows Server 2008 R2
- Microsoft Windows Server 2012
- Microsoft Windows Server 2012 R2
- Microsoft Windows Storage Server 2008 R2 Essentials SP1
- Microsoft Windows Small Business Server 2003 (x86)
- Microsoft Windows Small Business Server 2003 R2 (x86)
- Microsoft Windows Small Business Server 2008 (x64)
- Microsoft Windows Small Business Server 2011 (x64)

La configuration matérielle dépend de la version du système d'exploitation utilisée. Il est recommandé de prendre connaissance de la documentation Microsoft Windows Server pour plus d'informations sur la configuration matérielle.

1.2 Types de protection

Il existe deux types de protection :

- Protection antivirus
- Protection antispyware

La protection antivirus et antispyware est l'une des fonctions de base d'ESET File Security. Cette protection vous prémunit des attaques contre le système en contrôlant les échanges de fichiers et de messages, ainsi que les communications Internet. Si une menace comportant un code malveillant est détectée, le module Antivirus peut l'éliminer en la bloquant dans un premier temps, puis en nettoyant, en supprimant ou en mettant en quarantaine l'objet infecté.

1.3 Interface utilisateur

ESET File Security dispose d'une interface utilisateur graphique très intuitive. Elle permet d'accéder très facilement aux principales fonctions du programme.

Outre l'interface utilisateur principale, une **arborescence de configuration avancée** est accessible depuis tous les emplacements du programme par l'intermédiaire de la touche F5.

Lorsque vous appuyez sur la touche F5, la fenêtre de l'arborescence de configuration avancée apparaît et affiche la liste des fonctions du programme qui peuvent être configurées. Depuis cette fenêtre, vous pouvez configurer les paramètres et les options en fonction de vos besoins. L'arborescence est divisée en deux sections : **Protection du serveur** et **Protection de l'ordinateur**. La partie **Protection du serveur** contient des exclusions automatiques qui sont propres au système d'exploitation du serveur et aux fichiers système. La partie **Protection de l'ordinateur** contient les éléments configurables de la protection du serveur proprement dit.

2. Installation

Après l'achat d'ESET File Security, le programme d'installation peut être téléchargé à partir du site web d'ESET (www.eset.com) sous forme de package .msi.

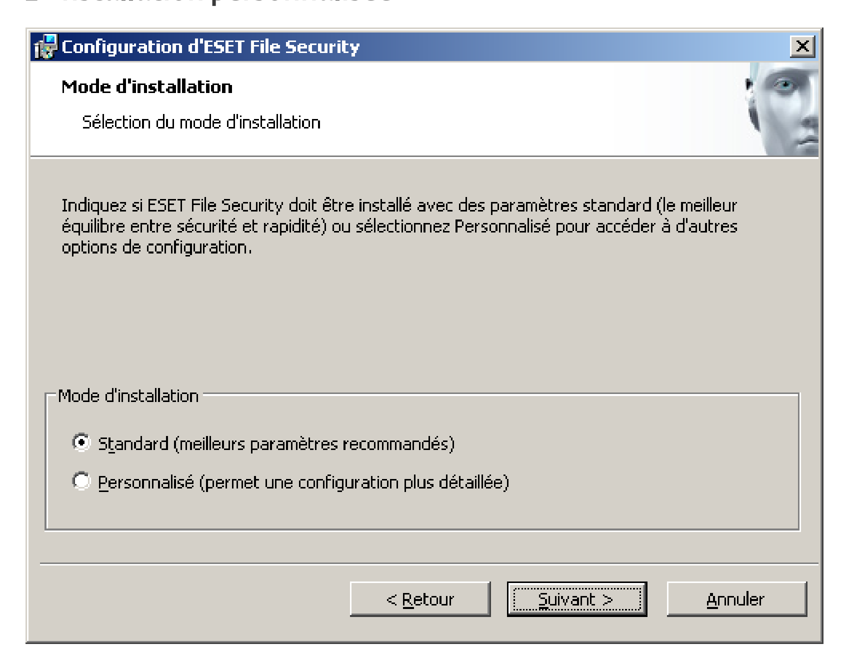
Veuillez noter que vous devez exécuter le programme d'installation avec le compte **Administrateur intégré**. Aucun autre utilisateur, même membre du groupe Administrateurs, ne disposera de droits d'accès suffisants. Vous devez donc utiliser un compte Administrateur intégré dans la mesure où vous ne parviendrez à effectuer l'installation avec aucun autre compte que **Administrateur**.

Il est possible d'exécuter le programme d'installation de deux façons :

- Vous pouvez vous connecter localement à l'aide des informations d'identification du compte Administrateur et simplement exécuter le programme d'installation
- Vous pouvez être connecté avec un autre compte d'utilisateur, mais vous devez ouvrir l'invite de commande avec **Exécuter en tant que...** et taper les informations d'identification du compte Administrateur pour que cmd s'exécute en tant qu'Administrateur, puis taper la command pour exécuter le programme d'installation (ex. `msiexec /i efsw_nt64_ENU.msi` mais vous devez remplacer `efsw_nt64_ENU.msi` par le nom de fichier précis du programme d'installation msi que vous avez téléchargé)

Lancez le programme d'installation ; l'assistant d'installation vous guide dans les opérations de configuration de base. Deux types d'installation sont disponibles, avec différents niveaux de détails de configuration :

1. **Installation standard**
2. **Installation personnalisée**



REMARQUE : Il est fortement recommandé, dans la mesure du possible, d'installer ESET File Security sur un système d'exploitation récemment installé et configuré. Toutefois, si vous n'avez pas besoin de l'installer sur un système existant, la meilleure solution consiste à désinstaller la version antérieure de ESET File Security, de redémarrer le serveur et d'installer ensuite la nouvelle version de ESET File Security.

2.1 Installation standard

Le mode d'installation standard installe rapidement ESET File Security avec la configuration minimale pendant l'installation. L'installation standard est le mode d'installation par défaut ; elle est recommandée si vous n'avez pas encore d'exigence particulière pour certains paramètres. Après l'installation d'ESET File Security sur le système, vous pouvez modifier les options et les paramètres de configuration à tout moment. Ce guide de l'utilisateur décrit les paramètres et les fonctionnalités en détail. Le mode d'installation standard offre un excellent système de sécurité très facile à utiliser et des performances système très élevées.

Après avoir sélectionné le mode d'installation et cliqué sur Suivant, vous êtes invité à entrer votre nom d'utilisateur et votre mot de passe. Ces informations jouent un rôle très important dans la protection permanente de votre système, car le nom d'utilisateur et le mot de passe permettent les mises à jour automatiques de la base des

signatures de virus.

Saisissez dans les champs correspondants le nom d'utilisateur et le mot de passe que vous avez reçus après l'achat ou l'enregistrement de votre produit. Si votre nom d'utilisateur et votre mot de passe ne sont pas disponibles, vous pouvez les indiquer ultérieurement directement dans le programme.

Dans la prochaine étape, **Gestionnaire de licences**, ajoutez le fichier de licence fourni par courrier électronique après l'achat de votre produit.

La dernière étape consiste à configurer le système d'alerte anticipé ThreatSense.Net. Le système d'avertissement anticipé ThreatSense.Net contribue à garantir qu'ESET est immédiatement et continuellement informé des nouvelles infiltrations dans le but de protéger ses clients. Le système permet de soumettre les nouvelles menaces au laboratoire de recherche sur les menaces d'ESET, où elles sont analysées, traitées puis ajoutées à la base des signatures de virus. Par défaut, l'option **Activer le système d'alerte anticipé ThreatSense.Net** est sélectionnée. Cliquez sur **Configuration avancée...** pour modifier les paramètres détaillés de soumission de fichiers suspects.

L'étape suivante de l'installation consiste à configurer la **Détection des applications potentiellement indésirables** . Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur le comportement du système d'exploitation. Reportez-vous au chapitre Applications potentiellement indésirables pour plus d'informations.

Ces applications sont souvent associées à d'autres programmes et peuvent être difficiles à remarquer lors de l'installation. Ces applications affichent habituellement une notification pendant l'installation, mais elles peuvent facilement s'installer sans votre consentement.

Sélectionnez l'optio **Activer la détection des applications potentiellement indésirables** pour autoriser ESET File Security à détecter ce type d'applications. Si vous ne souhaitez pas utiliser cette fonctionnalité, sélectionnez l'option **Désaciver la détection des applications potentiellement indésirables.**

La dernière étape de l'installation standard consiste à confirmer l'installation en cliquant sur le bouton **Installer**.

2.2 Installation personnalisée

L'installation personnalisée est destinée aux utilisateurs qui souhaitent configurer ESET File Security pendant l'installation.

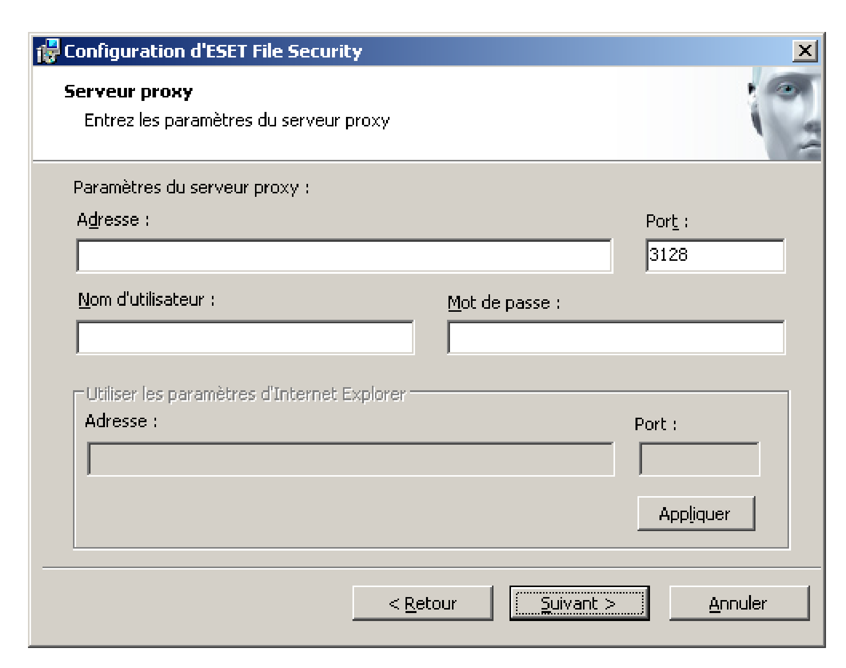
Après avoir sélectionné le mode d'installation et cliqué sur **Suivant**, vous êtes invité à sélectionner un emplacement de destination pour l'installation. Par défaut, le programme s'installe dans le dossier *C:\Program Files\ESET\ESET File Security*. Cliquez sur **Parcourir...** pour changer d'emplacement (non recommandé).

Entrez ensuite votre **nom d'utilisateur** et votre **mot de passe**. Cette étape est la même que dans l'installation standard (reportez-vous à Installation standard).

Dans la prochaine étape **Gestionnaire de licences**, ajoutez le fichier de licence fourni par courrier électronique après l'achat de votre produit.

Après avoir entré le nom d'utilisateur et le mot de passe, cliquez sur **Suivant** pour passer à l'étape **Configurez votre connexion Internet**.

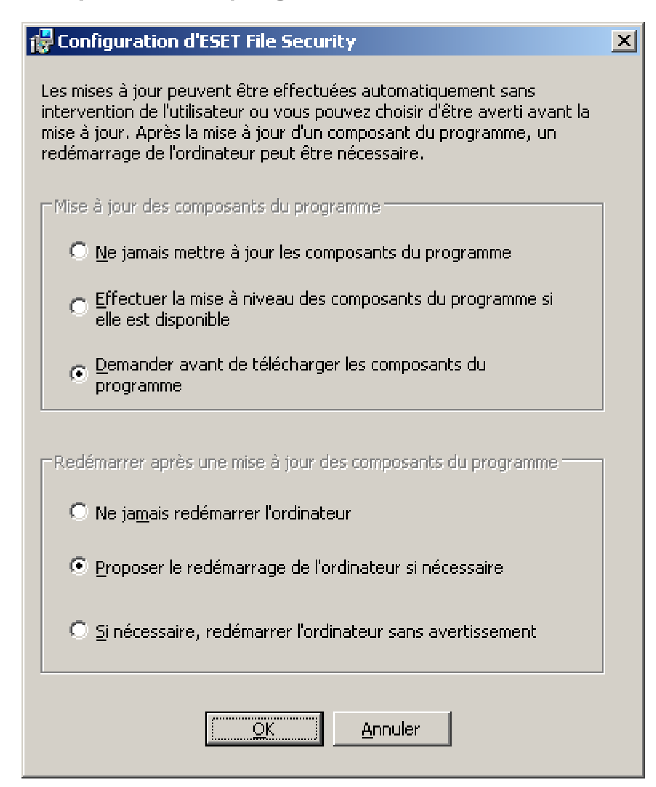
Si vous utilisez un serveur proxy, ce dernier doit être configuré correctement pour que les mises à jour des signatures de virus fonctionnement correctement. Si vous souhaitez utiliser un serveur proxy configuré automatiquement, sélectionnez le paramètre par défaut **Je ne sais pas si ma connexion Internet utilise un serveur proxy. Utiliser les mêmes paramètres qu'Internet Explorer (Recommandé)** et cliquez sur **Suivant**. Si vous n'utilisez pas de serveur proxy, sélectionnez l'option **Je n'utilisse pas de serveur proxy**.



Si vous préférez indiquer les informations détaillées du serveur proxy par vous-même, vous pouvez configurer les paramètres du serveur proxy manuellement. Pour configurer les paramètres du serveur proxy, sélectionnez l'option **J'utilise un serveur proxy** et cliquez sur **Suivant**. Entrez l'adresse IP ou l'adresse URL de votre serveur proxy dans le champ **Adresse**. Dans le champ **Port**, spécifiez le port sur lequel le serveur proxy accepte les connexions (3128 par défaut). Si le serveur proxy exige une authentification, saisissez un **nom d'utilisateur** et un **mot de passe** pour accorder l'accès au serveur proxy. Les paramètres du serveur proxy peuvent être copiés depuis Internet Explorer. Une fois les détails du serveur proxy entrés, cliquez sur **Appliquer** et confirmez la sélection.

Cliquez sur **Suivant** pour passer à l'étape **Configurez les paramètres de mise à jour automatique**. Cette étape permet d'indiquer la façon dont les mises à jour des composants programme sont gérées sur le système. Cliquez sur **Changer...** pour accéder aux paramètres avancés.

Si vous ne voulez pas que les composants du programme soient mis à jour, sélectionnez l'option **Ne jamais mettre à jour les composants du programme**. L'option **Demander avant de télécharger les composants du programme** affiche une fenêtre de confirmation avant le téléchargement des composants du programme. Pour télécharger les mises à niveau des composants du programme, sélectionnez l'option **Toujours mettre à jour les composants du programme**.



REMARQUE : le redémarrage du système est généralement nécessaire après la mise à jour des composants du programme. Il est recommandé de sélectionner l'option **Ne jamais redémarrer**. Les dernières mises à jour des

composants entrent en vigueur au redémarrage suivant du serveur (qu'il soit planifié, manuel ou autre). Vous pouvez sélectionner l'option **Proposer de redémarrer si nécessaire** si vous souhaitez que le système vous rappelle de redémarrer le serveur après la mise à jour des composants. Avec ce paramètre, vous pouvez redémarrer le serveur immédiatement ou ultérieurement.

La fenêtre suivante de l'installation permet d'indiquer un mot de passe afin de protéger les paramètres du programme. Sélectionnez l'option **Protéger les paramètres de configuration par mot de passe** et choisissez un mot de passe à indiquer dans les champs **Nouveau mot de passe** et **Confirmer le nouveau mot de passe**.

Les deux étapes d'installation suivantes, **Activer le système d'alerte anticipé ThreatSense.Net et Détection des applications potentiellement indésirables** sont identiques aux étapes de l'installation standard (reportez-vous à « Installation standard »).

Cliquez sur **Installer** dans la fenêtre **Prêt à installer** pour terminer l'installation.

2.3 Terminal Server

Si vous avez installé ESET File Security sur un serveur Windows agissant comme Terminal Server, vous souhaiterez peut-être désactiver l'interface utilisateur graphique ESET File Security afin d'empêcher son démarrage à chaque connexion de l'utilisateur. Reportez-vous au chapitre Désactivation de l'interface utilisateur graphique sur Terminal Server pour accéder aux étapes de désactivation.

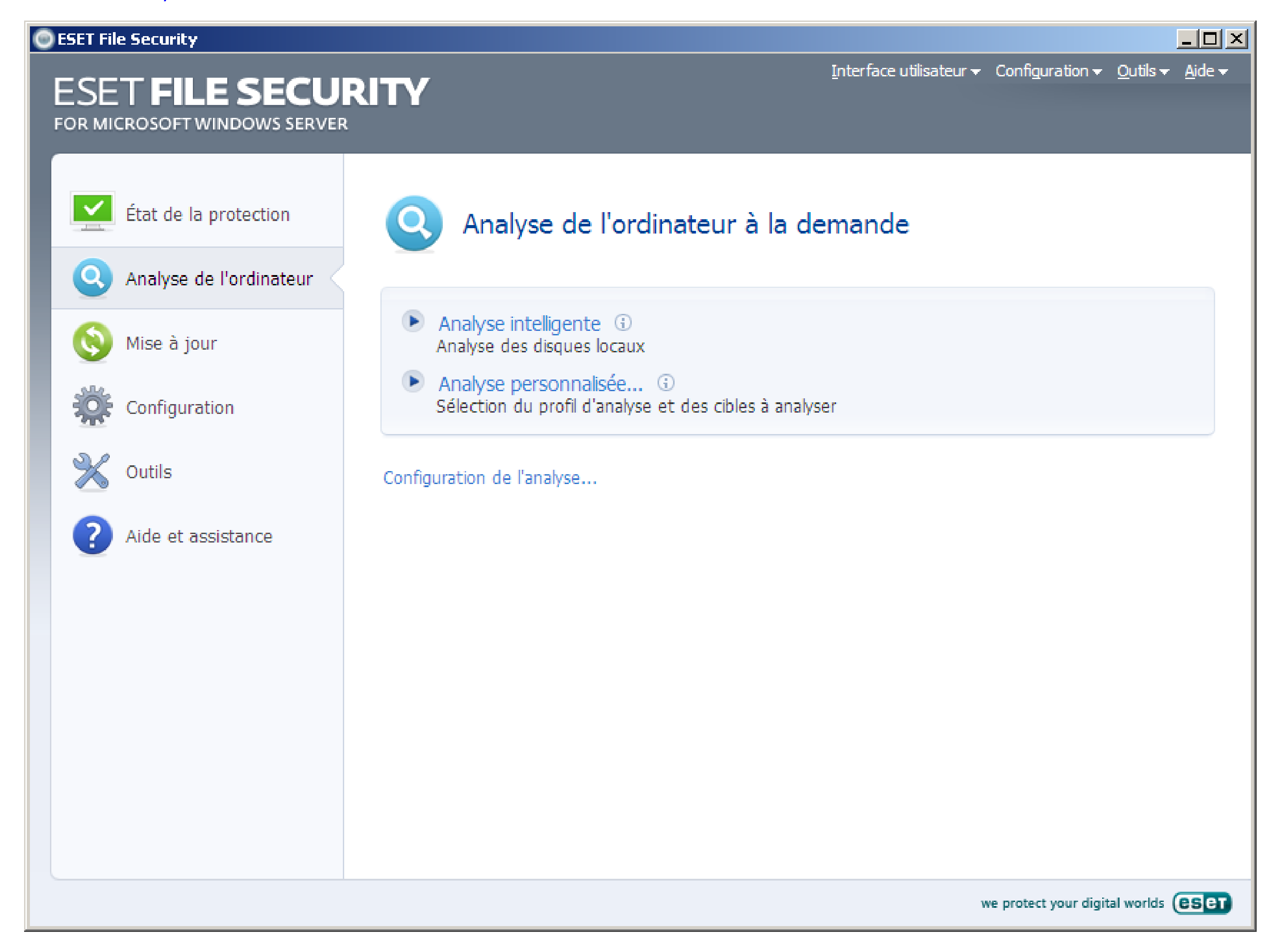
2.4 Mise à niveau vers une version plus récente

Les nouvelles versions d'ESET File Security offrent des améliorations ou apportent des solutions aux problèmes que les mises à jour automatiques des modules ne pouvaient pas résoudre. La mise à niveau vers une nouvelle version peut s'effectuer de l'une des manières suivantes :

1. Mise à niveau automatique par l'intermédiaire d'une mise à jour des composants du programme
   Dans la mesure où les mises à jour des composants du programme sont distribuées à tous les utilisateurs et peuvent avoir un impact sur certaines configurations système, elles sont mises à disposition après de longues périodes de test afin que la mise à niveau s'effectue sans difficulté sur toutes les configurations système. Si vous devez effectuer la mise à niveau vers une nouvelle version dès qu'elle est disponible, utilisez l'une des méthodes suivantes.
2. Effectuez une mise à niveau manuelle en téléchargeant la nouvelle version et en l'installant sur l'installation précédente.
   Au début de l'installation, vous pouvez choisir de conserver les paramètres du programme en cochant la case **Utiliser les paramètres actuels**.
3. Effectuez une mise à niveau manuelle avec déploiement automatique sur un réseau par l'intermédiaire d'ESET Remote Administrator.

2.5 Analyse de l'ordinateur à la demande

Après l'installation d'ESET File Security, vous devez effectuer une analyse de l'ordinateur afin de rechercher tout code malveillant éventuel. Dans la fenêtre principale du programme, cliquez sur **Analyse de l'ordinateur**, puis sur **Analyse intelligente**. Pour plus d'informations sur l'analyse de l'ordinateur à la demande, reportez-vous à la section Analyse de l'ordinateur à la demande.



3. Guide du débutant

Ce chapitre donne un premier aperçu d'ESET File Security et de ses paramètres de base.

3.1 Présentation de l'interface utilisateur

La fenêtre principale d'ESET File Security est divisée en deux sections principales. La fenêtre principale de droite affiche les informations correspondant à l'option sélectionnée dans le menu principal à gauche.

Voici une description des options disponibles dans le menu principal :

État de la protection : fournit des informations sur l'état de protection d'ESET File Security. Si l'option Mode avancé est activée, les sous-menus **Regarder l'activité** et **Statistiques** apparaissent.

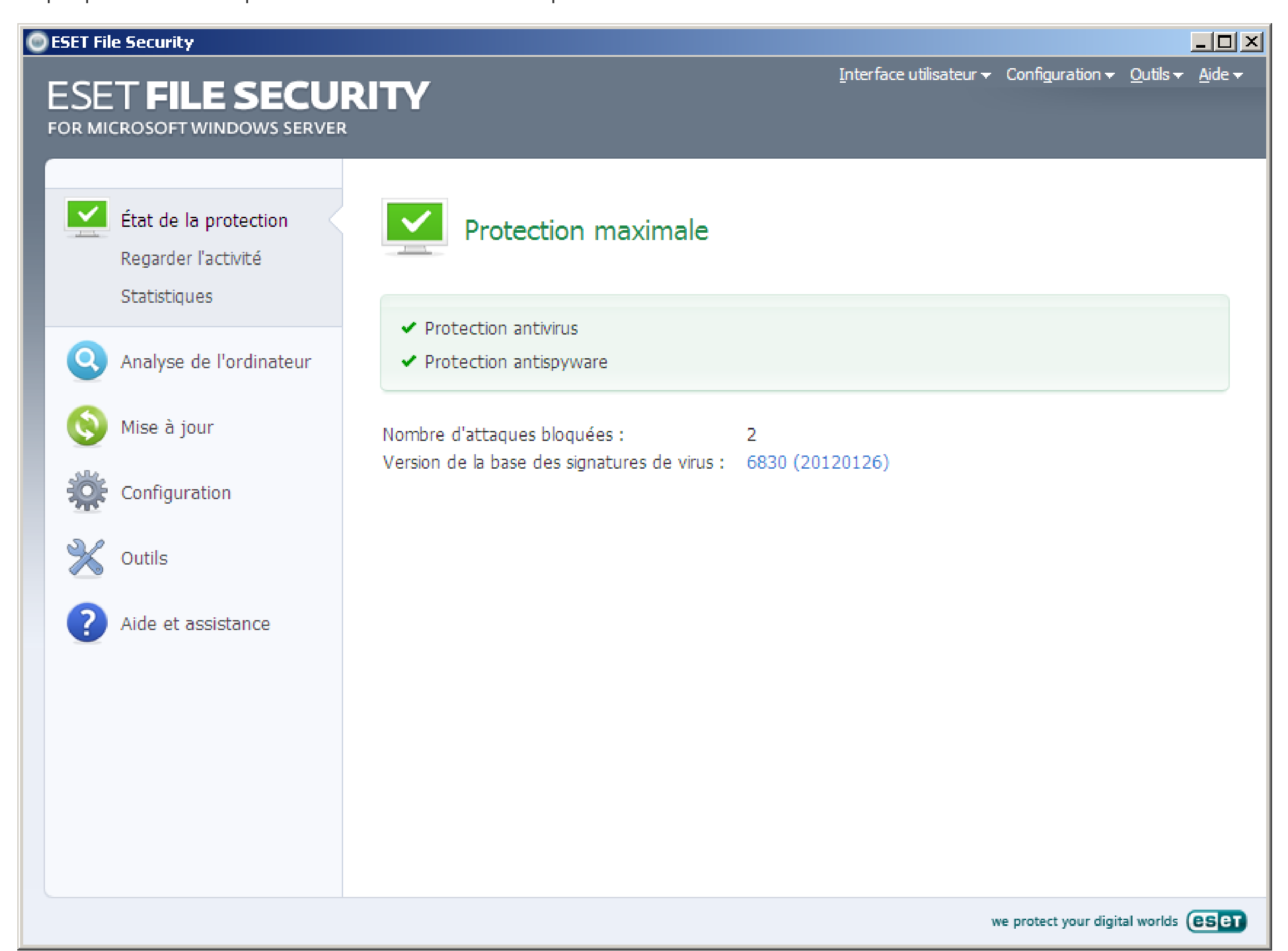
Analyse de l'ordinateur : cette option permet de configurer et de lancer l'analyse de l'ordinateur à la demande.

Mettre à jour : affiche des informations sur les mises à jour de la base des signatures de virus.

Configuration : sélectionnez cette option pour ajuster le niveau de sécurité de votre ordinateur. Si l'option Mode avancé est activée, le sous-menu **Antivirus et antispyware** apparaît.

Outils : permet d'accéder aux fichiers journaux, aux **fichiers journaux**, à la **quarantaine**, au **planificateur** et à **SysInspector**. Cette option n'apparaît qu'en mode avancé.

Aide et assistance- : permet d'accéder aux fichiers d'aide, à la base de connaissances ESET, au site Internet d'ESET, et propose des liens permettant d'ouvrir une requête à l'assistance client.



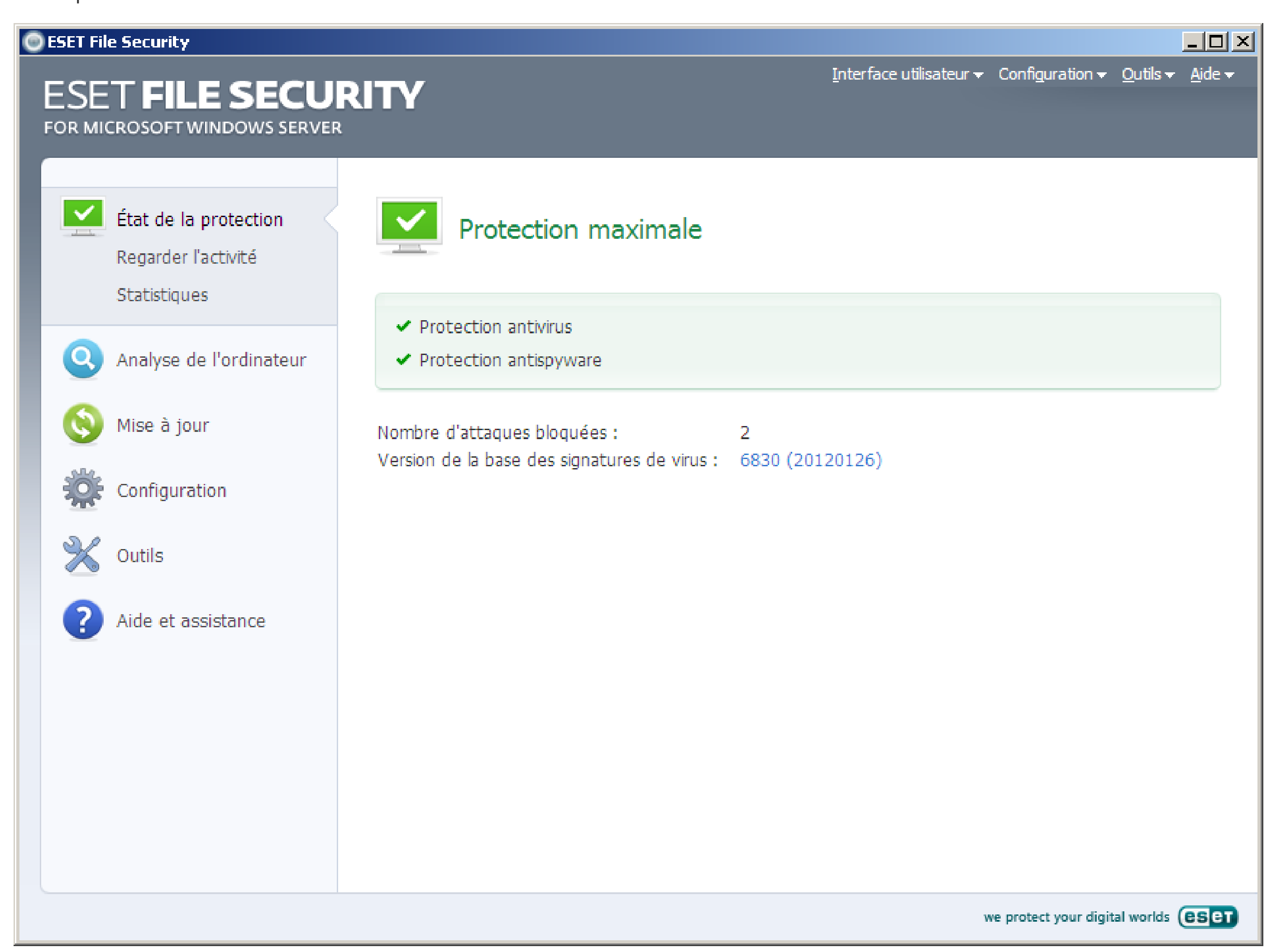
3.1.1 Contrôle du fonctionnement du système

Pour afficher l'**état de la protection**, cliquez sur l'option en haut du menu principal. La fenêtre principale affiche un résumé de l'état de fonctionnement d'ESET File Security et un sous-menu avec deux options apparaît : **Regarder l'activité** et **Statistiques**. Sélectionnez l'une de ces options pour afficher des informations détaillées sur votre système.

Lorsque ESET File Security fonctionne correctement, l'**état de protection** apparaît en vert. Dans les autres cas, l'état apparaît en orange ou en rouge, ce qui signifie que le programme nécessite votre attention.

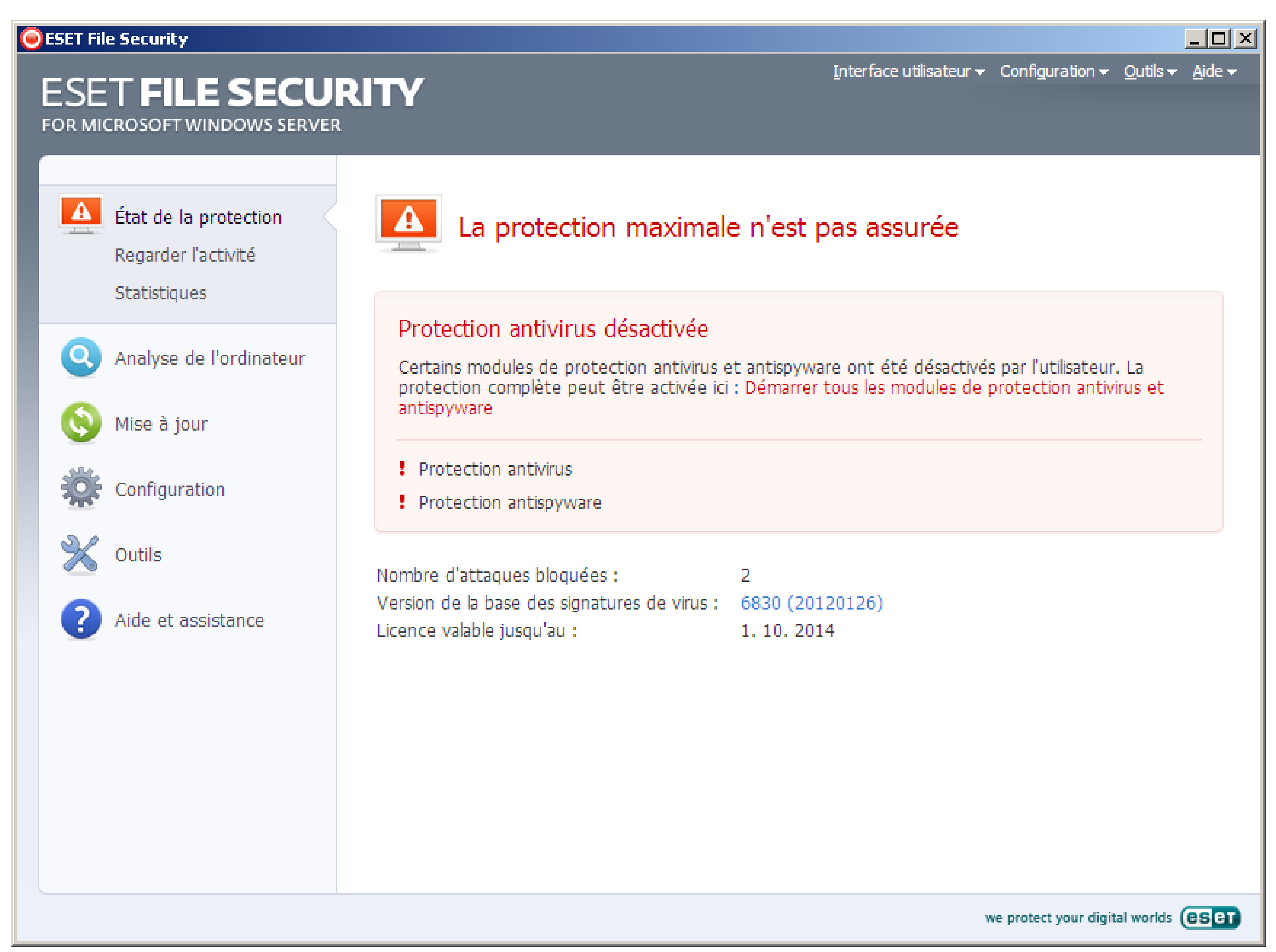
En cliquant sur l'option de sous-menu **Regarder l'activité**, vous pouvez observer l'activité en cours du système de fichier sous forme de graphique en temps réel (axe horizontal). L'axe vertical représente les données lues (ligne bleue) et les données écrites (ligne rouge).

Le sous-menu **Statistiques** permet d'afficher le nombre d'objets infectés, nettoyés et propres d'un module défini. Vous pouvez choisir différents modules dans la liste déroulante.



3.1.2 Que faire lorsque le programme ne fonctionne pas correctement ?

Une coche verte s'affiche en regard de chaque module activé et fonctionnant correctement. Dans le cas contraire, un point d'exclamation rouge ou orange et des informations supplémentaires sur le module s'affichent dans la partie supérieure de la fenêtre. Une suggestion de solution pour corriger le module est également affichée. Pour changer l'état des différents modules, cliquez sur **Configuration** dans le menu principal puis sur le module souhaité.



Si vous ne parvenez pas à résoudre le problème à l'aide des solutions suggérées, cliquez sur Aide et assistance pour accéder aux fichiers d'aide ou pour effectuer des recherches dans la base de connaissances. Si vous avez besoin d'aide, vous pouvez envoyer une requête à l'assistance client d'ESET. Le service client d'ESET répondra très rapidement à vos questions et vous permettra de déterminer une solution.

3.2 Configuration des mises à jour

La mise à jour de la base des signatures de virus et des composants du programme est un élément important de la protection totale contre les attaques des codes malveillants. Il faut donc accorder une grande attention à sa configuration et à son fonctionnement. Dans le menu principal, sélectionnez **Mise à jour** et cliquez sur **Mettre à jour la base des signatures de virus** dans la fenêtre principale afin de rechercher une éventuelle mise à jour de la base de données. **Configurer le nom d'utilisateur et le mot de passe...** affiche une boîte de dialogue dans laquelle vous devez entrer le nom d'utilisateur et le mot de passe (reçus lors de l'achat).

Si le nom d'utilisateur et le mot de passe ont été entrés pendant l'installation d'ESET File Security, vous ne serez pas invité à les réintroduire à ce stade.

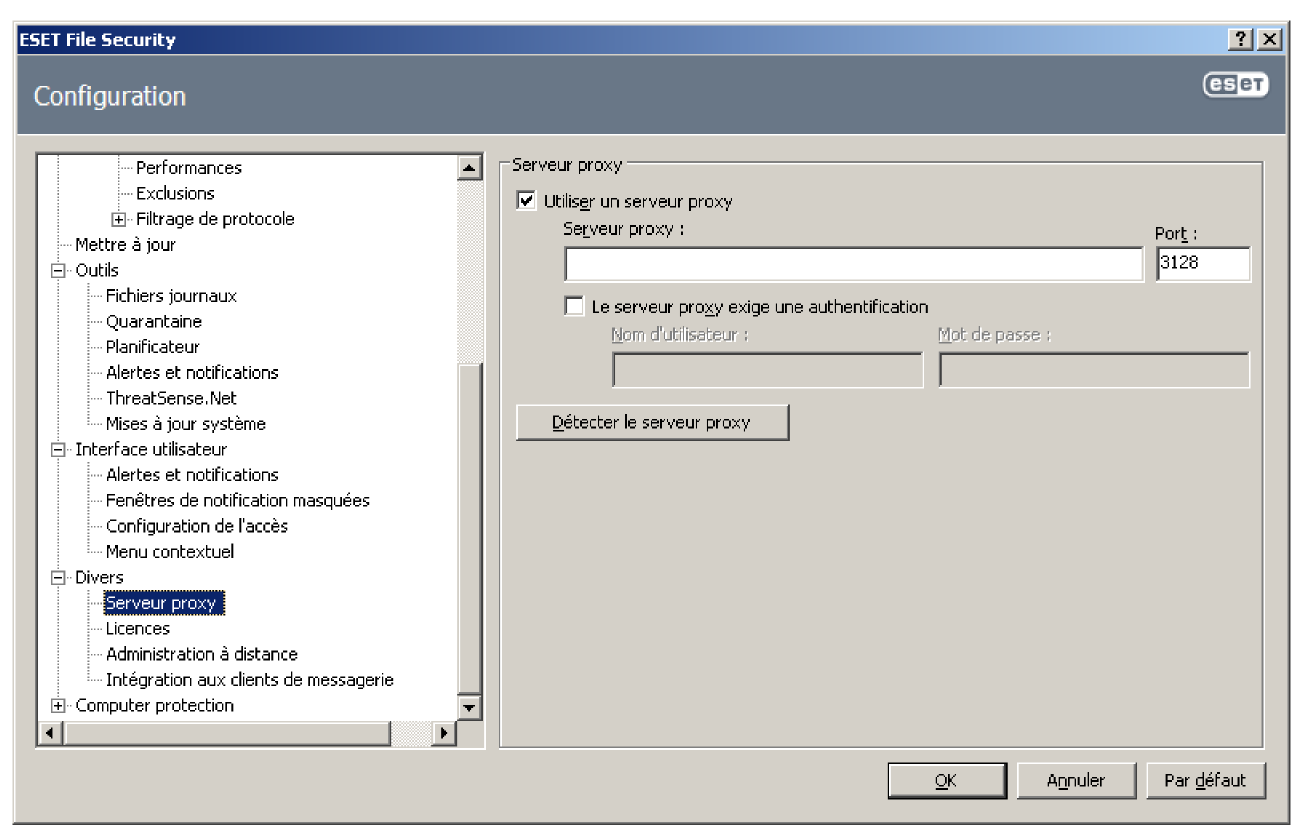


La fenêtre Configuration avancée (cliquez sur **Configuration** dans le menu principal, puis cliquez sur **Accéder à l'arborescence de la configuration avancée complète...** ou appuyez sur F5) contient des options supplémentaires de mise à jour. Cliquez sur **Mise à jour** dans l'arborescence de configuration avancée. Le menu déroulant **Serveur de mise à jour** : doit être configuré sur **Choisir automatiquement**. Pour configurer les options de mise à jour avancée tels que le mode de mise à jour, l'accès au serveur proxy, les connexions LAN et la création de copies de signatures de virus, cliquez sur le bouton **Configuration...**

ESET File Security
Configuration
Performances
Exclusions
Filtrage de protocole
Mettre à jour
Outils
Fichiers journaux
Quarantaine
Planificateur
Alertes et notifications
ThreatSense.Net
Mises à jour système
Interface utilisateur
Alertes et notifications
Fenêtres de notification masquées
Configuration de l'accès
Menu contextuel
Divers
Serveur proxy
Licences
Administration à distance
Intégration aux clients de messagerie
Computer protection
Profil sélectionné :
Mon profil
Profils...
Mettre à jour les paramètres du profil sélectionné
Serveur de mise à jour :
Choisir automatiquement
Modifier...
Nom d'utilisateur :
updv4
Mot de passe :
••••••••
Configuration avancée des mises à jour :
Configuration...
Effacer le cache de mise à jour :
Effacer
Ne pas afficher de notification de réussite de la mise à jour
OK
Annuler
Par défaut

3.3 Configuration du serveur proxy

Si vous utilisez un serveur proxy pour contrôler les connexions Internet sur un système utilisant ESET File Security, il doit être spécifié dans la configuration avancée. Pour accéder à la fenêtre de configuration du serveur proxy, appuyez sur la touche F5 pour ouvrir la fenêtre Configuration avancée et cliquez sur **Divers** > **Serveur proxy** dans l'arborescence de configuration avancée. Sélectionnez l'option **Utiliser un serveur proxy**, puis complétez les champs **Serveur proxy** (adresse IP) et **Port**. Si nécessaire, sélectionnez l'option **Le serveur proxy exige une authentification**, puis indiquez le **nom d'utilisateur** et le **mot de passe**.



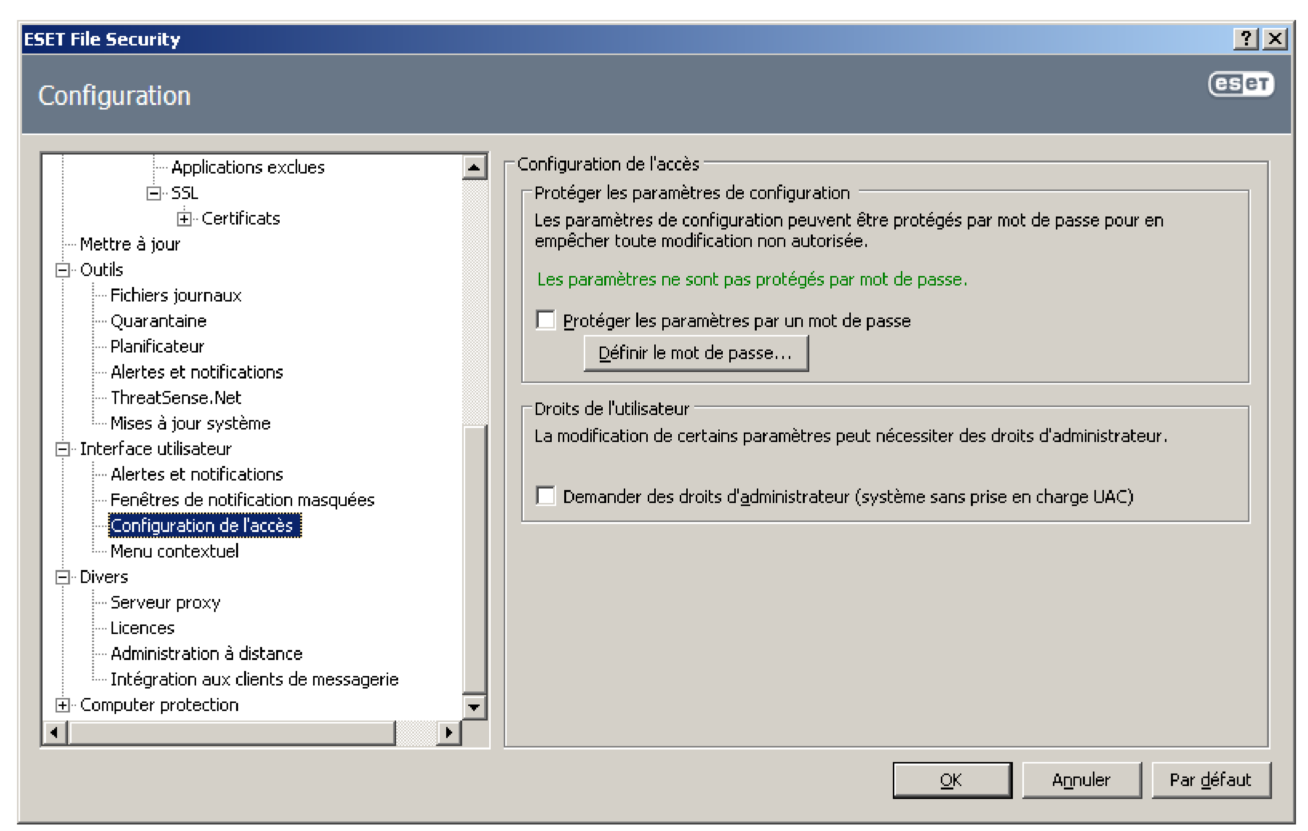
Si ces informations ne sont pas disponibles, vous pouvez essayer de détecter automatiquement les paramètres du serveur proxy en cliquant sur le bouton **Détecter le serveur proxy**.

REMARQUE : Les options du serveur proxy peuvent varier selon les profils de mise à jour. Si c'est le cas, configurez les différents profils de mise à jour dans Configuration avancée en cliquant sur **Mettre à jour** dans l'arborescence de configuration avancée.

3.4 Protection des paramètres

Les paramètres ESET File Security peuvent être très importants pour la stratégie de sécurité de votre organisation. Des modifications non autorisées peuvent mettre en danger la stabilité et la protection de votre système. Pour protéger les paramètres de configuration par mot de passe, cliquez dans le menu principal sur **Configuration** > **Accéder à l'arborescence de la configuration avancée complète...** > **Interface utilisateur** > **Configuration de l'accès** , sélectionnez l'option **Protection des paramètres par mot de passe** et cliquez sur le bouton **Définir le mot de passe...**

Saisissez un mot de passe dans les champs **Nouveau mot de passe** et **Confirmer le mot de passe**, puis cliquez sur **OK**. Vous aurez besoin de ce mot de passe pour les prochaines modifications de ESET File Security.



REMARQUE : Cliquez ici pour afficher la configuration à l'aide d'eShell.

4. Utilisation de ESET File Security

4.1 ESET File Security : protection du serveur

ESET File Security protège votre serveur grâce aux fonctionnalités essentielles suivantes : Antivirus et Antispyware, bouclier résident (protection en temps réel), protection de l'accès Web et protection du client de messagerie. Vous trouverez des informations sur chaque type de protection dans la section ESET File Security - Protection de l'ordinateur. En outre, une fonctionnalité intitulée Exclusions automatiques est disponible. Cette fonctionnalité identifie les applications serveur et les fichiers du système d'exploitation serveur critiques, puis les ajoute automatiquement à la liste des exclusions. Cette fonctionnalité réduira le risque de conflits potentiels et augmentera les performances globales du serveur lors de l'exécution du logiciel antivirus.

4.1.1 Exclusions automatiques

Les développeurs d'applications et de systèmes d'exploitation serveur recommandent d'exclure des analyses antivirus les ensembles de dossiers et fichiers de travail critiques pour la plupart de leurs produits. Les analyses antivirus peuvent avoir une influence négative sur les performances d'un serveur, ce qui peut provoquer des conflits et même empêcher l'exécution de certaines applications sur le serveur. Les exclusions permettent de réduire le risque de conflits potentiels et d'augmenter les performances globales du serveur lors de l'exécution du logiciel antivirus.

ESET File Security identifie les applications serveur et les fichiers du système d'exploitation serveur critiques, puis les ajoute automatiquement à la liste des exclusions. Une fois ajouté à la liste, le processus/l'application serveur peut être activé (option par défaut) ou désactivé en sélectionnant/désélectionnant la case appropriée, ce qui donne le résultat suivant :

1) Si l'exclusion d'une application/d'un système d'exploitation reste activée, les fichiers et dossiers critiques correspondants sont ajoutés à la liste des fichiers exclus de l'analyse (**Configuration avancée** > **Protection de l'ordinateur** > **Antivirus et antispyware** > **Exclusions**). À chaque redémarrage du serveur, le système vérifie automatiquement les exclusions et restaure celles qui auraient pu être supprimées de la liste. Ce paramètre est recommandé si vous souhaitez vous assurer que les exclusions automatiques conseillées sont toujours appliquées.

2) Si l'exclusion d'une application/d'un système d'exploitation est désactivée, les fichiers et dossiers critiques correspondants restent dans la liste des fichiers exclus de l'analyse (**Configuration avancée** > **Protection de l'ordinateur** > **Antivirus et antispyware** > **Exclusions**). Toutefois, ils ne sont pas vérifiés et renouvelés automatiquement dans la liste **Exclusions** à chaque redémarrage du serveur (reportez-vous au point 1 ci-dessus). Ce paramètre est recommandé pour les utilisateurs avancés qui souhaitent supprimer ou modifier certaines des exclusions standard. Si vous souhaitez supprimer les exclusions de la liste sans redémarrer le serveur, vous devez les supprimer de la liste manuellement (**Configuration avancée** > **Protection de l'ordinateur** > **Antivirus et antispyware** > **Exclusions)**.

Toutes les exclusions définies par l'utilisateur et saisies manuellement dans **Configuration avancée** > **Protection de l'ordinateur** > **Antivirus et antispyware** > **Exclusions** ne sont pas concernées par les paramètres décrits ci-dessus.

Les exclusions automatiques des applications/systèmes d'exploitation serveur sont sélectionnées en fonction des recommandations de Microsoft. Pour plus d'informations, utilisez les liens suivants :

http://support.microsoft.com/kb/822158
http://support.microsoft.com/kb/245822
http://support.microsoft.com/kb/823166
http://technet.microsoft.com/fr-fr/library/bb332342(EXCHG.80).aspx
http://technet.microsoft.com/fr-fr/library/bb332342.aspx

4.2 ESET File Security : protection de l'ordinateur

ESET File Security fournit tous les outils nécessaires à la protection du serveur en tant qu'ordinateur. Cette solution protège efficacement pour votre serveur grâce aux types de protection suivants : Antivirus et Antispyware, bouclier résident (protection en temps réel), protection de l'accès Web et protection du client de messagerie.

4.2.1 Antivirus et antispyware

La protection antivirus vous prémunit des attaques contre le système en contrôlant les échanges de fichiers et de courrier, ainsi que les communications Internet. Si une menace comportant du code malveillant est détectée, le module antivirus peut l'éliminer en la bloquant dans un premier temps, puis en nettoyant, en supprimant ou en mettant en quarantaine l'objet infecté.

4.2.1.1 Protection en temps réel du système de fichiers

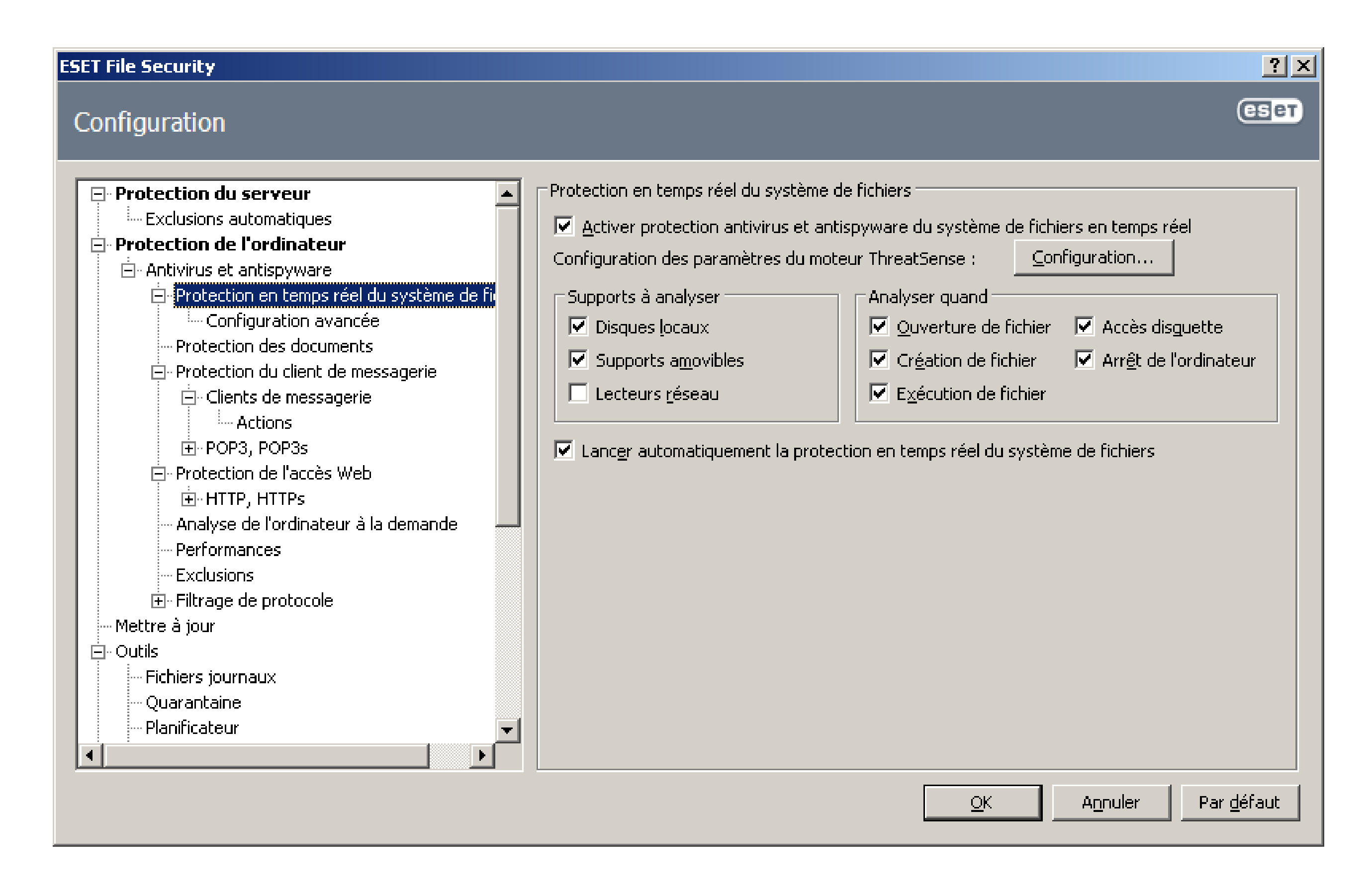
La protection en temps réel du système de fichiers contrôle tous les événements liés à l'antivirus dans le système. Elle analyse tous les fichiers à la recherche de code malveillant lors de l'ouverture, de la création ou de l'exécution de ces fichiers sur l'ordinateur. La protection en temps réel du système de fichiers est lancée au démarrage du système.

4.2.1.1.1 Configuration du contrôle

La protection en temps réel du système de fichiers vérifie tous les types de supports et le contrôle est déclenché par différents événements. Lors de l'utilisation des méthodes de détection de la technologie ThreatSense (décrites dans la section Configuration des paramètres du moteur ThreatSense), la protection du système de fichiers en temps réel est différente pour les nouveaux fichiers et pour les fichiers existants. Pour les nouveaux fichiers, il est possible d'appliquer un niveau de contrôle plus approfondi.

Pour réduire l'impact de la protection en temps réel sur le système, les fichiers déjà analysés ne sont pas analysés plusieurs fois (sauf s'ils ont été modifiés). Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base des signatures de virus. Ce comportement est configuré à l'aide de l'optimisation intelligente. Si cette fonction est désactivée, tous les fichiers sont analysés à chaque accès. Pour modifier cette option, ouvrez la fenêtre Configuration avancée et cliquez sur **Antivirus et antispyware** > **Protection en temps réel du système de fichiers** dans l'arborescence de configuration avancée. Cliquez ensuite sur le bouton **Configuration...** à côté de l'option **Configuration des paramètres du moteur ThreatSense**, cliquez sur **Autre** et sélectionnez ou désélectionnez l'option **Activer l'optimisation intelligente**.

Par défaut, la protection en temps réel est lancée au démarrage du système d'exploitation, assurant ainsi une analyse ininterrompue. Dans certains cas (par exemple en cas de conflit avec un autre analyseur en temps réel), il est possible de mettre fin à la protection en temps réel en désactivant l'option **Lancer automatiquement la protection en temps réel du système de fichiers**.



4.2.1.1.1.1 Supports à analyser

Par défaut, tous les types de supports font l'objet de recherches de menaces potentielles.

Disques locaux : contrôle tous les disques durs système.

Supports amovibles : disquettes, périphériques USB, etc.

Disques réseau : analyse tous les lecteurs mappés.

Nous recommandons de conserver les paramètres par défaut et de ne les modifier que dans des cas spécifiques, par exemple lorsque l'analyse de certains supports ralentit de manière significative les transferts de données.

4.2.1.1.1.2 Analyser quand (analyse déclenchée par un événement)

Par défaut, tous les fichiers sont analysés lors de leur ouverture, création ou exécution. Il est recommandé de conserver les paramètres par défaut, car ils offrent le niveau maximal de protection en temps réel pour votre ordinateur.

L'option **Accès disquette** contrôle le secteur d'amorçage des disquettes lors de l'accès au lecteur. L'option **Arrêt de l'ordinateur** contrôle les secteurs d'amorçage du disque dur lors de l'arrêt de l'ordinateur. Bien que les virus d'amorçage soient rares de nos jours, il est recommandé de laisser ces options activées, car le risque existe toujours d'une infection par un virus d'amorçage provenant d'autres sources.

4.2.1.1.1.3 Options d'analyse avancées

Vous trouverez des options de configuration détaillées dans **Protection de l'ordinateur** > **Antivirus et antispyware** > **Protection en temps réel du système de fichiers** > **Configuration avancée**.

Autres paramètres ThreatSense pour les fichiers nouveaux et modifiés - La probabilité d'infection dans les nouveaux fichiers ou les fichiers modifiés est comparativement supérieure à celle des fichiers existants.. C'est la raison pour laquelle le programme vérifie ces fichiers avec des paramètres d'analyse supplémentaires. Outre les méthodes d'analyse basées sur les signatures, l'heuristique avancée est utilisée, ce qui améliore sensiblement les taux de détection. Outre les nouveaux fichiers, l'analyse porte également sur les fichiers auto-extractibles (.sfx) et les fichiers exécutables compressés (en interne). Par défaut, les archives sont analysées jusqu'au dixième niveau d'imbrication et sont contrôlées indépendamment de leur taille réelle. Désactivez l'option Paramètres d'analyse d'archive par défaut pour modifier les paramètres d'analyse d'archive.

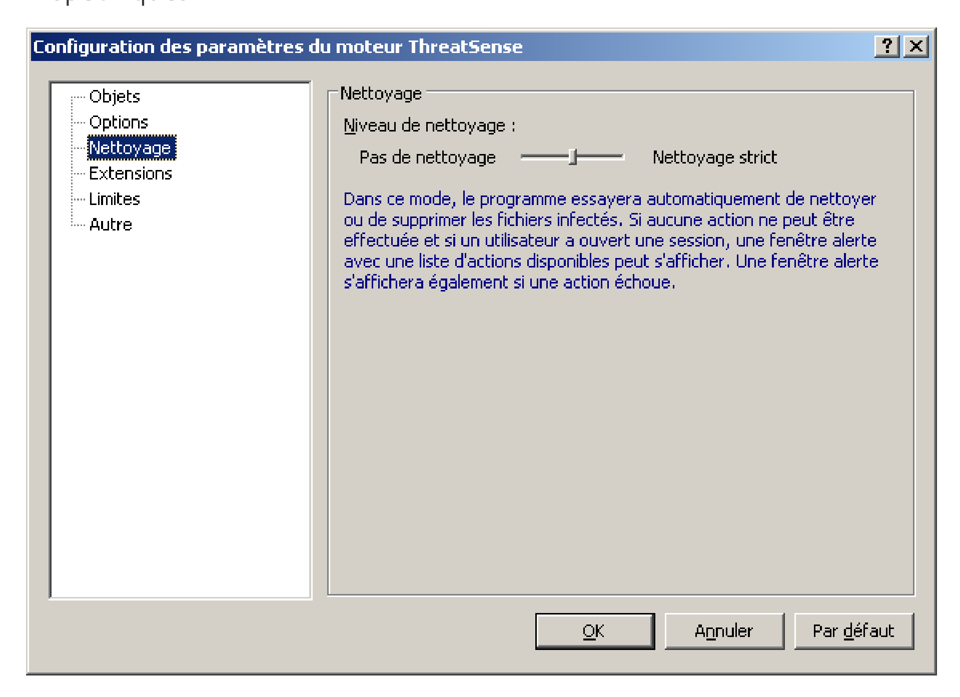
Autres paramètres ThreatSense.Net pour les fichiers exécutés : par défaut, l'heuristique avancée n'est pas

utilisée lors de l'exécution des fichiers.. Toutefois, vous souhaiterez dans certains cas activer cette option (en cochant l'option **Heuristique avancée à l'exécution du fichier**). Notez que l'heuristique avancée peut ralentir l'exécution de certains programmes en raison de la charge système accrue.

4.2.1.1.2 Niveaux de nettoyage

La protection en temps réel offre trois niveaux de nettoyage. Pour sélectionner un niveau de nettoyage, cliquez sur le bouton **Configuration...** dans la section **Protection en temps réel du système de fichiers**, puis cliquez sur la branche **Nettoyage**.

- Le premier niveau, **Pas de nettoyage**, affiche une fenêtre d'avertissement qui propose des options pour chaque infiltration détectée. L'utilisateur doit choisir une action pour chaque infiltration. Ce niveau est conçu pour les utilisateurs expérimentés qui connaissent les actions à entreprendre en cas d'infiltration.
- Le niveau par défaut choisit et exécute automatiquement une action prédéfinie (selon le type d'infiltration). La détection et la suppression d'un fichier infecté sont signalées par un message affiché dans l'angle inférieur droit de l'écran. Les actions automatiques ne sont pas réalisées si l'infiltration se trouve dans une archive (qui contient également des fichiers intacts) ou si les objets infectés n'ont pas d'action prédéfinie.
- Le troisième niveau, **Nettoyage strict**, est le plus « agressif » : tous les fichiers infectés sont nettoyés. Ce niveau pouvant éventuellement entraîner la perte de fichiers valides, il n'est recommandé que dans des situations spécifiques.



4.2.1.1.3 Quand faut-il modifier la configuration de la protection en temps réel

La protection en temps réel est le composant essentiel de la sécurisation du système. Il faut donc procéder avec prudence lors de la modification des paramètres de ce module. Il est recommandé de ne modifier les paramètres que dans des cas très précis. Ce peut être le cas notamment lorsqu'il y a conflit avec une autre application ou avec l'analyseur en temps réel d'un autre logiciel antivirus.

Après l'installation d'ESET File Security, tous les paramètres sont optimisés pour garantir aux utilisateurs le niveau maximum de sécurité du système. Pour rétablir les paramètres par défaut, cliquez sur le bouton **Par défaut** situé dans la partie inférieure droite de la fenêtre **Protection en temps réel du système de fichiers** (**Configuration avancée** > **Antivirus et antispyware** > **Protection en temps réel du système de fichiers**).

4.2.1.1.4 Vérification de la protection en temps réel

Pour vérifier que la protection en temps réel fonctionne et détecte les virus, utilisez un fichier de test d'eicar.com. Ce fichier de test est un fichier spécial inoffensif, détectable par tous les programmes antivirus. Le fichier a été créé par la société EICAR (European Institute for Computer Antivirus Research) et permet de tester la fonctionnalité des programmes antivirus. Le fichier eicar.com est téléchargeable depuis http://www.eicar.org/download/eicar.com

REMARQUE : avant d'effectuer une vérification de la protection en temps réel, vous devez désactiver le pare-feu. S'il est activé, il détecte le fichier et empêche le téléchargement des fichiers de test.

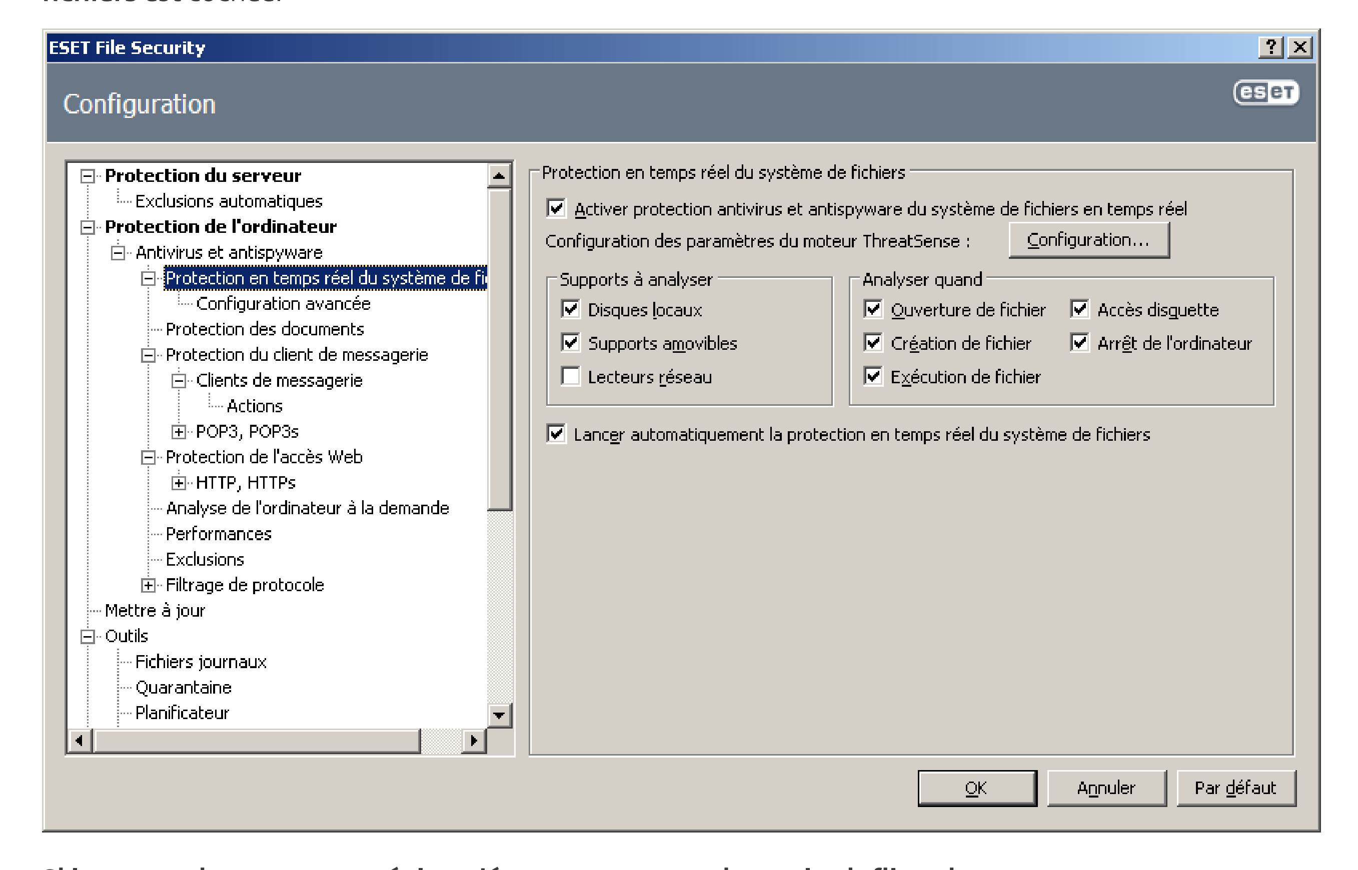
4.2.1.1.5 Que faire si la protection en temps réel ne fonctionne pas ?

Dans le chapitre suivant, nous décrivons des problèmes qui peuvent survenir lors de l'utilisation de la protection en temps réel, ainsi que la façon de les résoudre.

La protection en temps réel est désactivée

Si la protection en temps réel a été désactivée par mégarde par un utilisateur, elle doit être réactivée. Pour réactiver la protection en temps réel, sélectionnez **Configuration** > **Antivirus et antispyware** et cliquez sur **Activer dans la** section **Protection en temps réel du système de fichiers** dans la fenêtre principale du programme.

Si la protection en temps réel ne se lance pas au démarrage du système, c'est probablement dû au fait que l'option **Lancement automatique de la protection en temps réel du système de fichiers est désactivée**. Pour activer cette option, sélectionnez Configuration avancée (F5) et cliquez sur **Protection en temps réel du système de fichiers** dans l'arborescence de configuration avancée. Dans la section **Configuration avancée** dans la partie inférieure de la fenêtre, vérifiez que la case **Lancer automatiquement la protection en temps réel du système de fichiers** est cochée.



Si la protection en temps réel ne détecte et ne nettoie pas les infiltrations

Assurez-vous qu'aucun autre programme antivirus n'est installé sur votre ordinateur. Si deux programmes de protection en temps réel sont activés en même temps, il peut y avoir un conflit entre les deux. Nous recommandons de désinstaller tout autre antivirus de votre système.

La protection en temps réel ne démarre pas

Si la protection en temps réel n'est pas lancée au démarrage du système (et si l'option **Lancer automatiquement la protection en temps réel du système de fichiers** est activée), le problème peut provenir de conflits avec d'autres programmes. Dans ce cas, consultez les spécialistes du service client ESET.

4.2.1.2 Protection du client de messagerie

La protection du courrier permet de contrôler la communication par courrier électronique effectuée via le protocole POP3. ESET File Security utilise le plugin pour Microsoft Outlook pour contrôler toutes les communications impliquant le client de messagerie (POP3, MAPI, IMAP, HTTP).

Lorsqu'il examine les messages entrants, le programme utilise toutes les méthodes d'analyse avancées offertes par le moteur d'analyse ThreatSense. Autrement dit, la détection des programmes malveillants s'effectue avant la comparaison avec la base des signatures de virus. L'analyse des communications via le protocole POP3 est indépendante du client de messagerie utilisé.

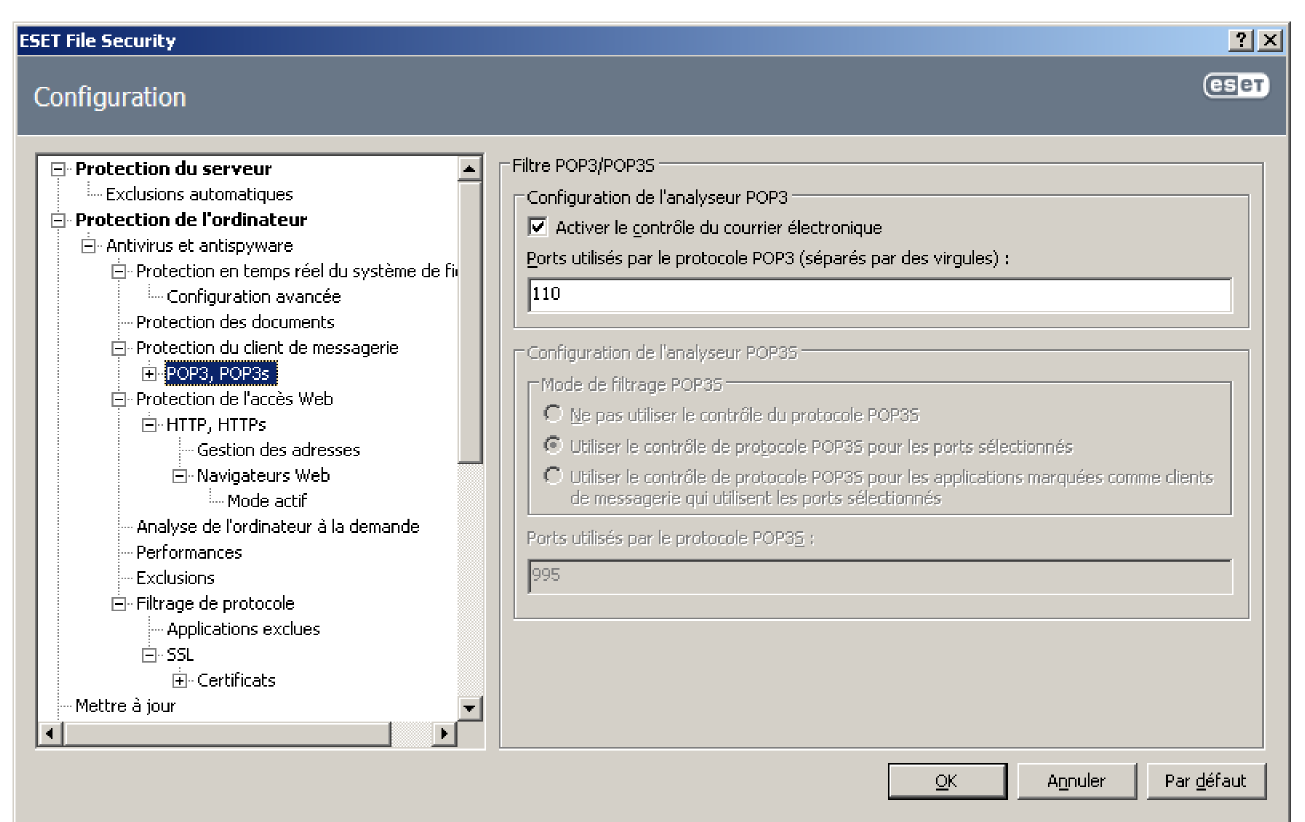
4.2.1.2.1 Contrôle POP3

Le protocole POP3 est le protocole le plus répandu pour la réception de messages dans un client de messagerie. ESET File Security protège ce protocole, quel que soit le client de messagerie utilisé.

Le module de protection qui assure ce contrôle est automatiquement lancé au démarrage du système d'exploitation et reste ensuite actif en mémoire. Pour que le module fonctionne correctement, assurez-vous qu'il est activé. Le contrôle POP3 s'effectue automatiquement sans qu'il faille reconfigurer le client de messagerie. Par défaut, toute communication sur le port 110 est soumise à une analyse, mais d'autres ports de communication peuvent être ajoutés au besoin. Les numéros de ports doivent être séparés par des virgules.

Les communications chiffrées ne sont pas contrôlées.

Pour utiliser le filtrage POP3/POP3S, vous devez activer d'abord le filtrage de protocole. Si les options POP3/POP3S sont grisées, sélectionnez **Protection de l'ordinateur** > **Antivirus et antispyware** > **Filtrage de protocole** depuis l'arborescence de configuration avancée et cochez l'option **Activer le filtrage du contenu des protocoles d'application**. Reportez-vous à la section Filtrage de protocole pour plus d'informations sur le filtrage et la configuration.



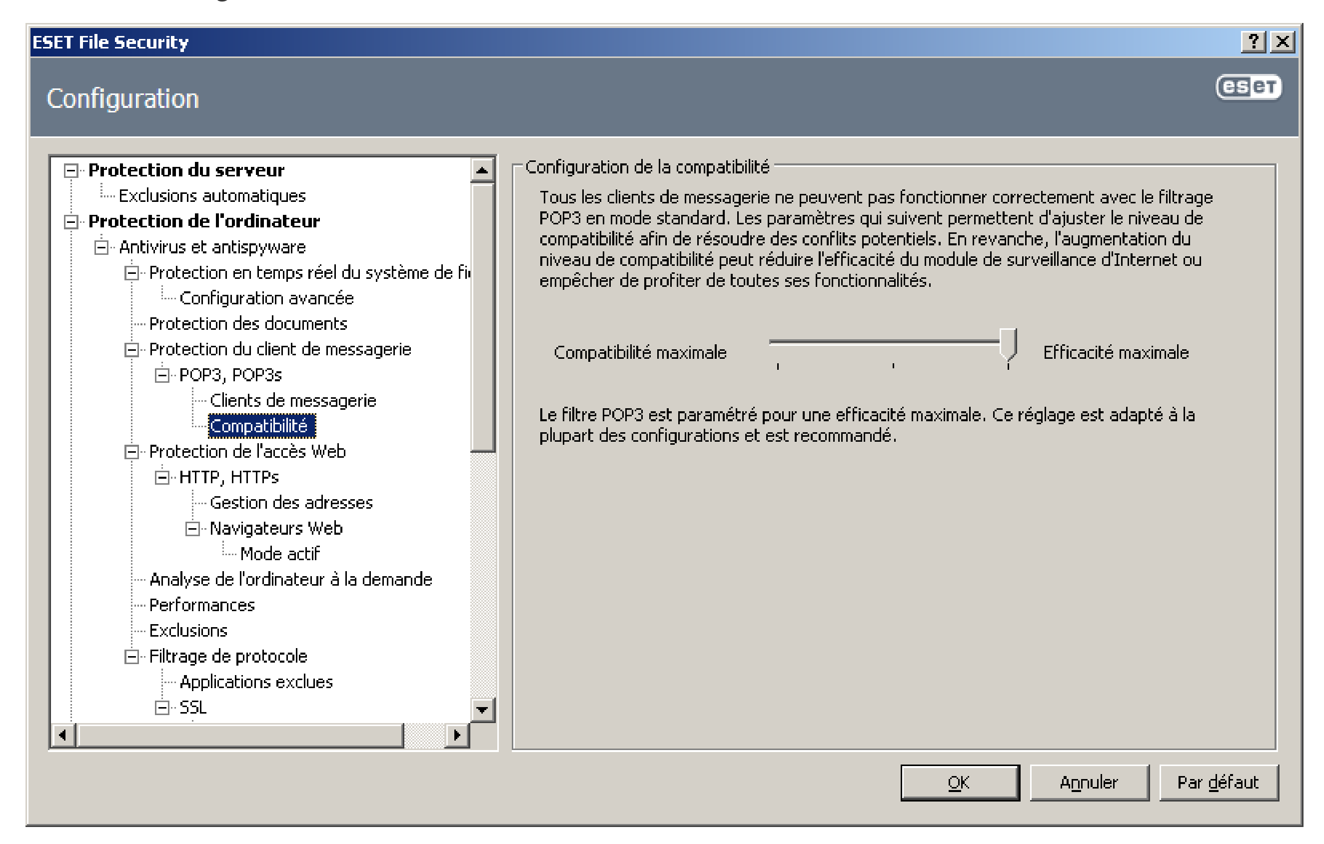
4.2.1.2.1.1 Compatibilité

Certains programmes de messagerie peuvent rencontrer des problèmes liés au filtrage POP3 (par exemple si vous recevez des messages sur une connexion Internet lente, la vérification peut entraîner des dépassements de délai). Dans ce cas, essayez de modifier la façon dont le contrôle est effectué. Une diminution du niveau de contrôle peut accélérer le processus de nettoyage. Pour ajuster le niveau de contrôle du filtrage POP3, sélectionnez, dans l'arborescence de configuration avancée, **Antivirus et antispyware** > **Protectiono du client de messagerie** > **POP3, POP3s** > **Compatibilité**.

Si l'option **Efficacité maximale** est activée, les infiltrations sont supprimées des messages infectés et les informations concernant l'infiltration sont insérées avant l'objet d'origine du message (les options **Supprimer** ou **Nettoyer** ou le niveau de nettoyage **Strict** ou **Par défaut** doivent être activés).

Une compatibilité moyenne modifie la façon dont les messages sont reçus. Les messages sont envoyés progressivement au client de messagerie. Une fois transféré, le message est analysé et les infiltrations sont recherchées. Avec ce niveau de contrôle, le risque d'infection est accru. Le niveau de nettoyage et la gestion des notifications (notes d'alerte ajoutées à l'objet et au corps des messages) sont identiques à ceux utilisés avec le paramètre d'efficacité maximale.

Avec le niveau de **compatibilité maximum**, vous êtes averti par l'affichage d'une fenêtre qui signale la réception d'un message infecté. Aucune information concernant les fichiers infectés n'est ajoutée à l'objet ni au corps des messages et les infiltrations ne sont pas supprimées automatiquement. Vous devez supprimer les infiltrations du client de messagerie.



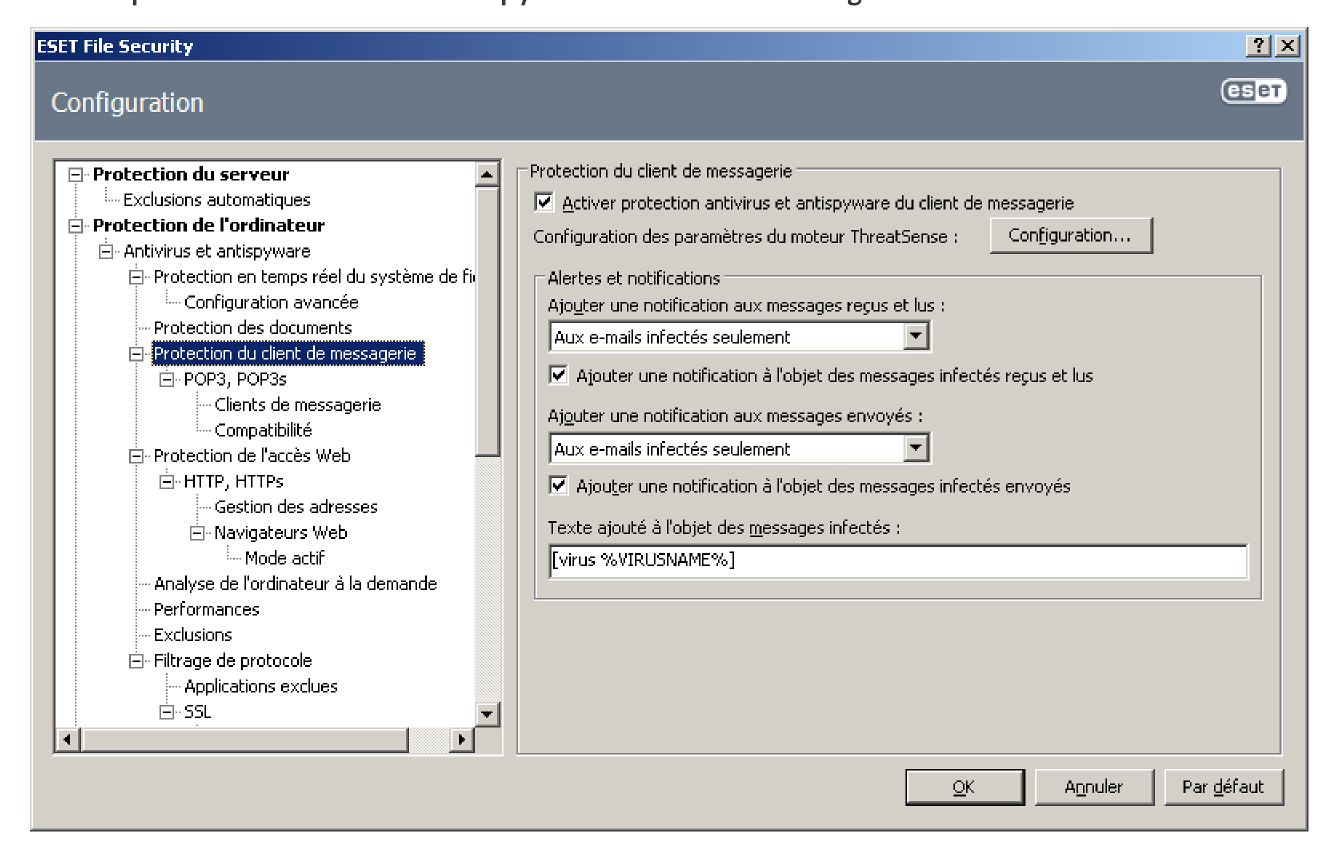
4.2.1.2.2 Intégration aux clients de messagerie

L'intégration d'ESET File Security aux clients de messagerie augmente le niveau de protection active contre les codes malveillants dans les messages électroniques. Si votre client de messagerie est pris en charge, cette intégration peut être activée dans ESET File Security. Si l'intégration est activée, la barre d'outils de protection antispam de ESET File Security est insérée directement dans le client de messagerie, ce qui permet de protéger les messages plus efficacement. Les paramètres d'intégration se trouvent dans la section **Configuration** > **Accéder à l'arborescence de la configuration avancée complète...** > **Divers** > **Intégration aux clients de messagerie**. L'intégration du client de messagerie permet d'activer l'intégration avec les clients de messagerie pris en charge. Les clients de messagerie pris en charge sont Microsoft Outlook, Outlook Express, Windows Mail, Windows Live Mail et Mozilla Thunderbird.

Sélectionnez l'option **Désactiver la vérification au changement de contenu de la boîte aux lettres** si vous constatez un ralentissement du système lors de l'utilisation du client de messagerie. Une telle situation peut se

présenter lors du téléchargement de messages à partir du magasin Kerio Outlook Connector.

Pour activer la protection de messagerie, cliquez sur **Configuration** > **Accéder à l'arborescence de configuration avancée complète...** > **Antivirus et antispyware** > **Protection du client de messagerie** et sélectionnez l'option **Activer protection antivirus et antispyware du client de messagerie**.



4.2.1.2.2.1 Ajout d'une notification au corps d'un courrier

Chaque courrier analysé par ESET File Security peut être marqué par l'ajout d'une notification à l'objet ou au corps du message. Cette fonction augmente la crédibilité du destinataire et, en cas de détection d'une infiltration, fournit des informations précieuses sur le niveau de menace d'un message ou d'un expéditeur.

Les options de cette fonctionnalité sont disponibles dans **Configuration avancée** > **Antivirus et antispyware** > **Protection du client de messagerie**. Vous pouvez sélectionner les options **Ajouter une notification aux messages reçus et lus** et **Ajouter une notification aux messages envoyés**. Vous pouvez également décider d'ajouter les notifications à tous les messages analysés, aux messages infectés uniquement ou à aucun des messages.

ESET File Security vous permet également d'ajouter des messages à l'objet d'origine des messages infectés. Pour activer l'ajout à l'objet, sélectionnez les options **Ajouter une notification à l'objet des messages infectés reçus et lus** et **Ajouter une notification à l'objet des messages infectés envoyés**.

Vous pouvez modifier le contenu des notifications dans le champ **Texte ajouté à l'objet des messages infectés**. Les modifications mentionnées précédemment permettent d'automatiser le filtrage des messages infectés, car elles vous permettent de filtrer des messages en fonction de leur objet (si votre client de messagerie prend en charge cette fonctionnalité) et de les placer dans un dossier distinct.

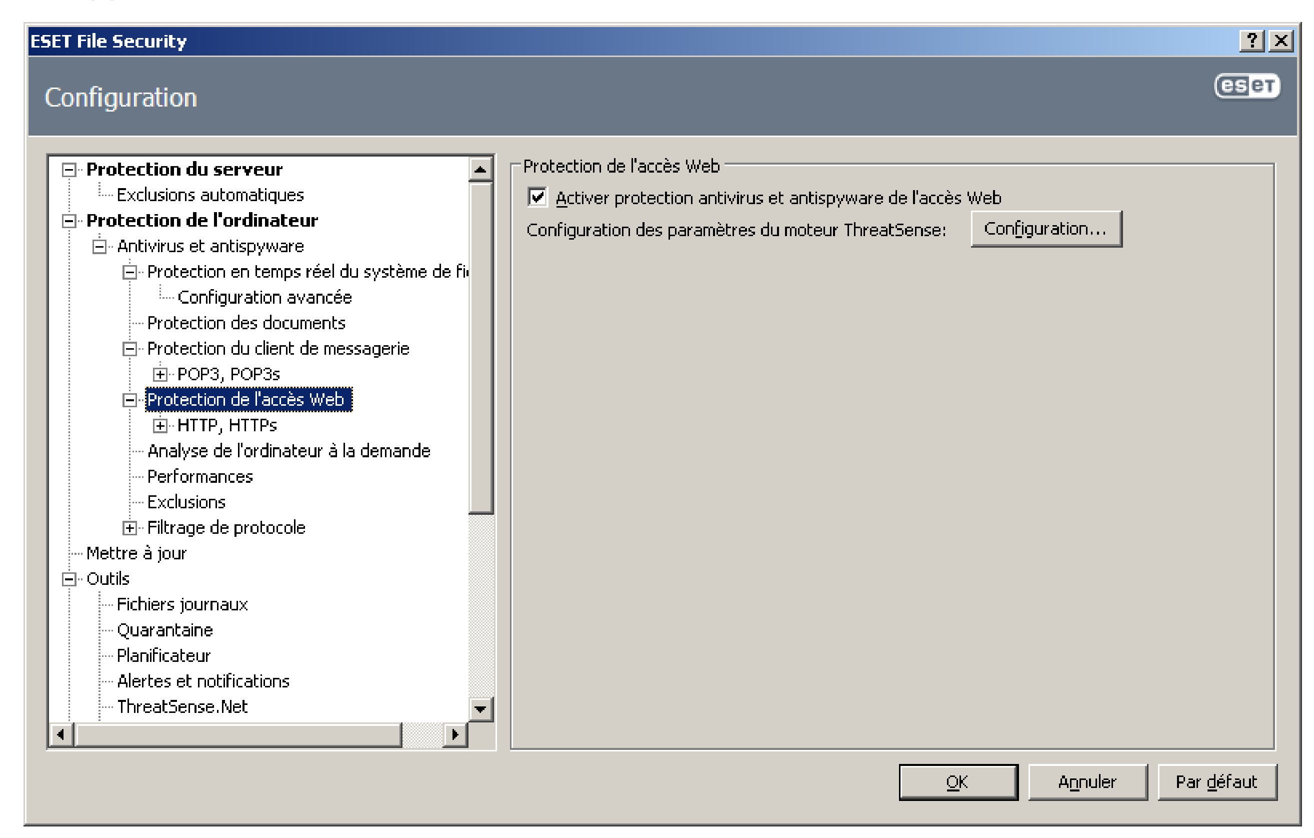
4.2.1.2.3 Suppression d'infiltrations

En cas de réception d'un message infecté, une fenêtre d'alerte s'affiche. Cette fenêtre indique le nom de l'expéditeur, son message et le nom de l'infiltration. La partie inférieure de la fenêtre présente les options disponibles concernant l'objet détecté : **Nettoyer**, **Supprimer** ou **Aucune action**. Dans la plupart des cas, nous recommandons de sélectionner **Nettoyer** ou **Supprimer**. Dans les situations particulières où vous souhaitez vraiment recevoir le fichier infecté, sélectionnez **Aucune action**.

Si le niveau **nettoyage strict** est activé, une fenêtre d'information sans options s'affiche.

4.2.1.3 Protection de l'accès Web

La connectivité Internet est une fonctionnalité standard des ordinateurs personnels. Elle est malheureusement devenue le principal mode de transfert des codes malveillants. Il est donc essentiel de surveiller de près la protection de l'accès à Internet. Il est vivement recommandé de sélectionner l'option **Afficher la notification de fin d'analyse dans une fenêtre séparée**. Cette option est disponible dans **Configuration avancée** (F5) > **Antivirus et antispyware** > **Protection de l'accès Web**.

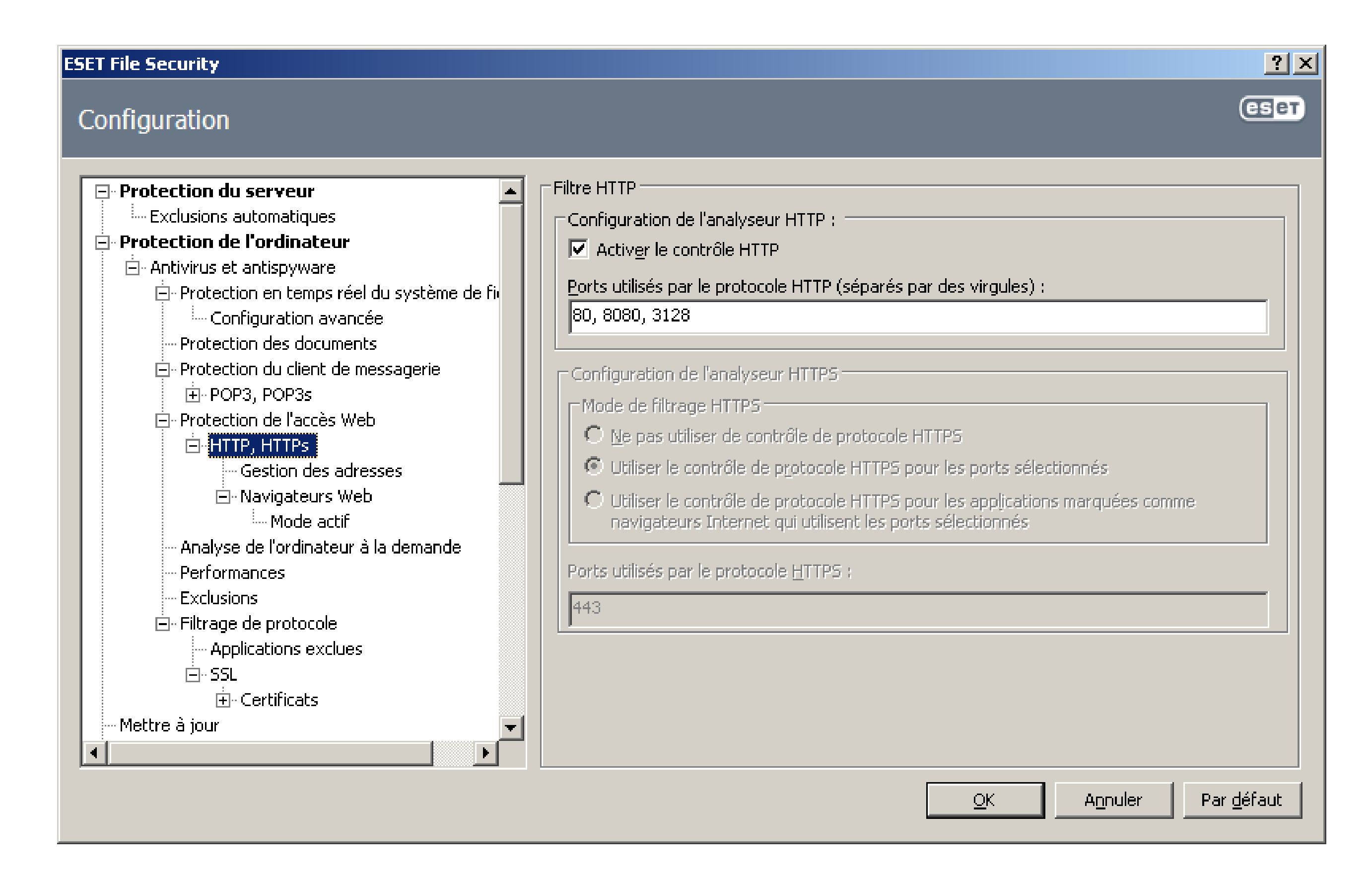


4.2.1.3.1 HTTP, HTTPs

La protection de l'accès Web opère par surveillance des communications entre les navigateurs Internet et les serveurs distants, conformément aux règles des protocoles HTTP et HTTPs (communications chiffrées). Par défaut, ESET File Security est configuré pour utiliser les normes de la plupart des navigateurs Internet. Toutefois, vous pouvez modifier les options de configuration de l'analyseur HTTP dans la section **Configuration avancée** (F5) > **Antivirus et antispyware** > **Protection de l'accès Web** > **HTTP, HTTPS**. Dans la fenêtre principale du filtre HTTP, vous pouvez activer ou désactiver l'option **Activer le contrôle HTTP**. Vous pouvez également définir les numéros de port utilisés pour la communication HTTP. Par défaut, les numéros de ports 80, 8080 et 3128 sont prédéfinis. Le contrôle HTTPs peut être effectué dans les modes suivants :

Ne pas utiliser de contrôle de protocole HTTPS : les communications chiffrées ne sont pas vérifiées.

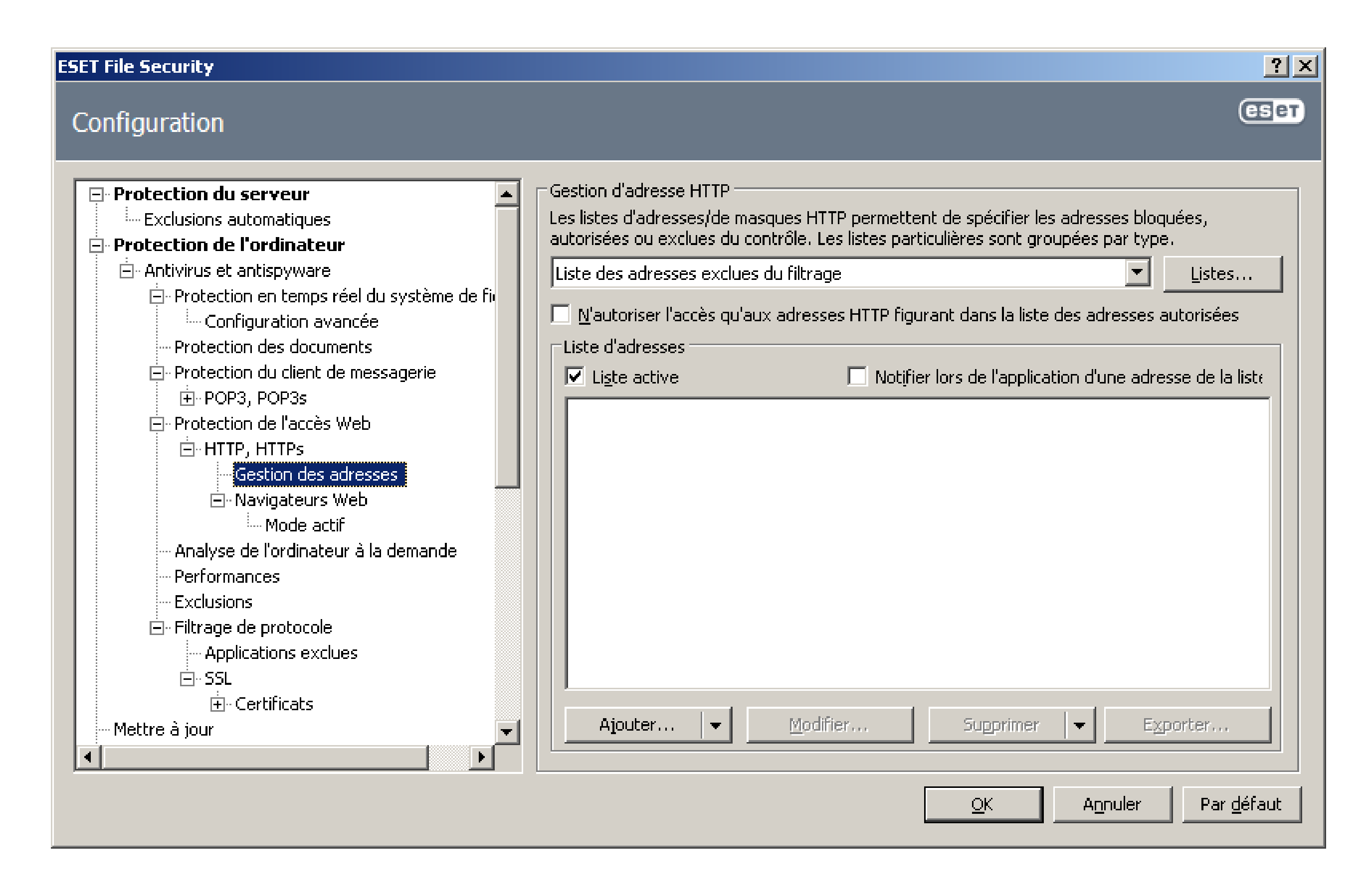
Utiliser le contrôle de protocole HTTPs pour les ports sélectionnés : le contrôle HTTPs n'a lieu que pour les ports définis dans **Ports utilisés par le protocole HTTPs**.



4.2.1.3.1.1 Gestion des adresses

Cette section permet de spécifier des listes d'adresses HTTP qui seront bloquées, autorisées ou exclues de la vérification. Les boutons **Ajouter...**, **Modifier...**, **Supprimer** et **Exporter...** permettent de gérer les listes d'adresses. Les sites Web figurant dans la liste des adresses bloquées ne seront pas accessibles. Les sites Web figurant dans la liste des adresses exclues sont accessibles sans aucune analyse de code malveillant. Si vous sélectionnez l'option **N'autoriser l'accès qu'aux adresses HTTP figurant dans la liste des adresses autorisées**, seules les adresses figurant dans la liste des adresses autorisées sont accessibles ; toutes les autres adresses HTTP sont bloquées.

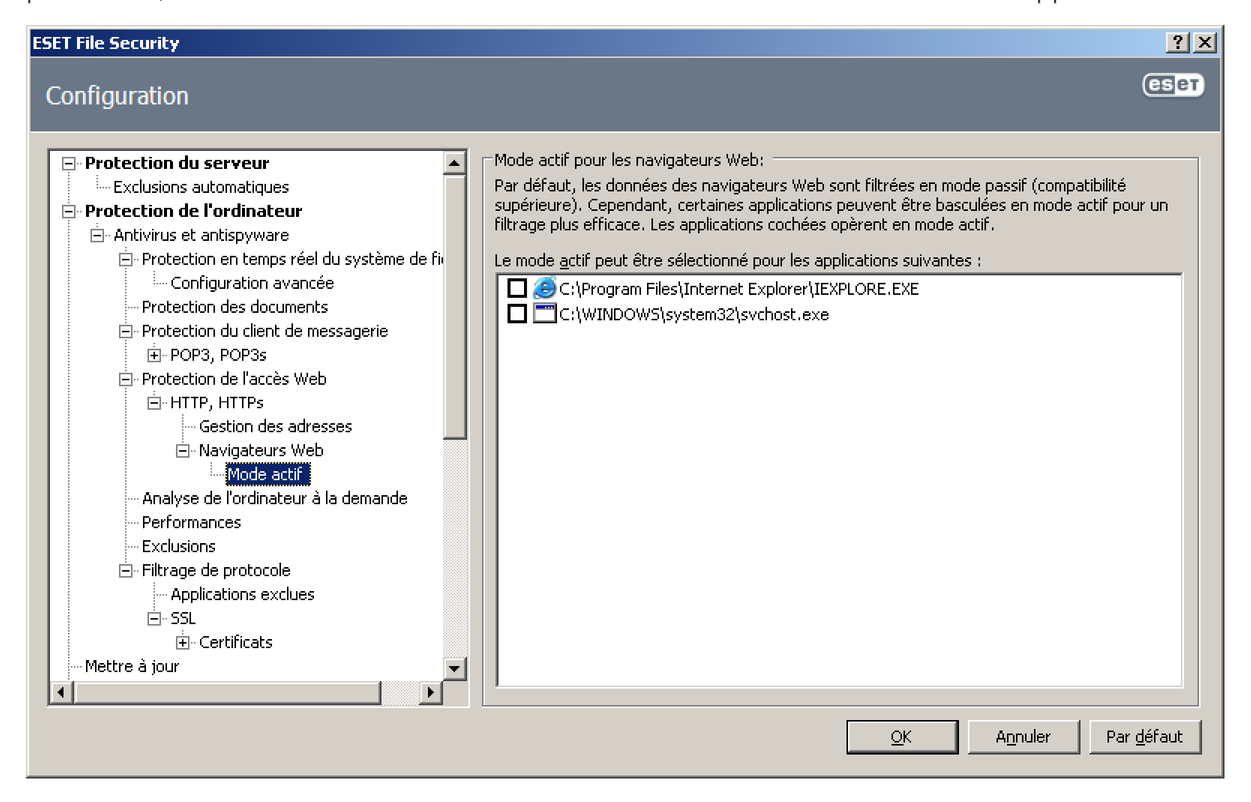
Dans toutes les listes, vous pouvez utiliser les symboles spéciaux « * » (astérisque) et « ? » (point d'interrogation). L'astérisque remplace n'importe quelle chaîne de caractères, tandis que le point d'interrogation remplace n'importe quel caractère. Un soin particulier doit être apporté à la spécification des adresses exclues, car la liste ne doit contenir que des adresses sûres et de confiance. De la même manière, veillez à employer correctement les symboles « * » et « ? » dans cette liste. Pour activer une liste, sélectionnez l'option **Liste active**. Pour être informé lors de l'entrée d'une adresse à partir de la liste actuelle, sélectionnez l'option **Notifier lors de l'application d'une adresse de la liste**.



4.2.1.3.1.2 Mode actif

La liste des applications comme étant des navigateurs Web est accessible directement depuis le sous-menu **Navigateurs Web** de la branche **HTTP, HTTPs**. Cette section contient également le sous-menu **Mode actif** qui définit le mode de contrôle des navigateurs Internet.

Avec le **Mode actif**, les données transférées sont examinées dans leur ensemble. Si l'option n'est pas activée, la communication des applications est contrôlée progressivement, par lots. La vérification des données est alors moins efficace, mais la compatibilité avec les applications répertoriées est meilleure. Si le Mode actif ne pose pas de problèmes, nous recommandons de l'activer en cochant la case située à côté de l'application souhaitée.



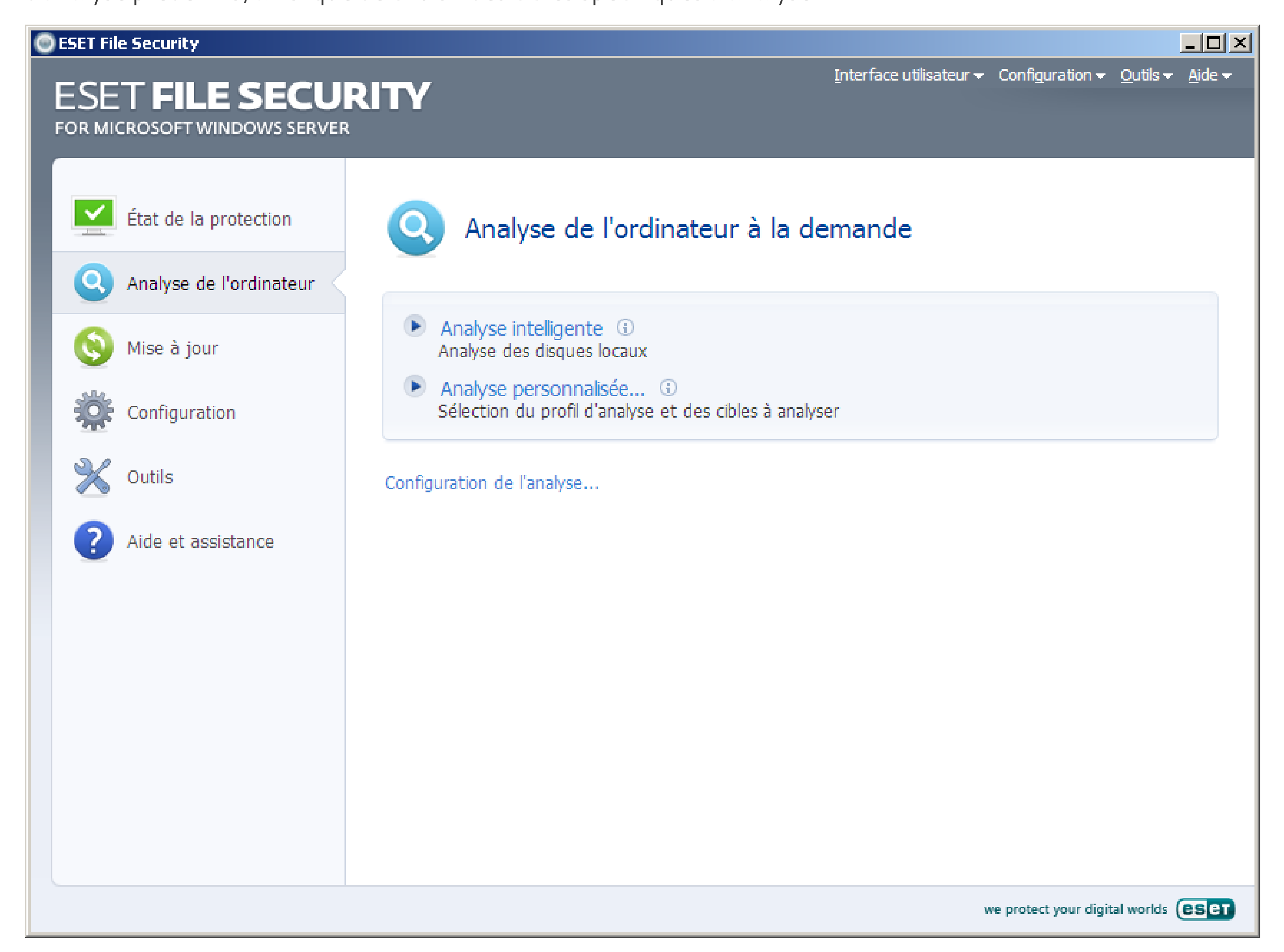
4.2.1.4 Analyse de l'ordinateur à la demande

Si vous pensez que votre ordinateur peut être infecté (en raison d'un comportement anormal), exécutez une analyse à la demande pour rechercher d'éventuelles infiltrations. Pour votre sécurité, il est essentiel que l'ordinateur soit analysé non seulement en cas de suspicion d'une infection, mais aussi régulièrement dans le cadre de mesures de sécurité routinières. Une analyse régulière peut détecter des infiltrations non détectées par l'analyseur en temps réel au moment de leur enregistrement sur le disque. Cela peut se produire si l'analyseur en temps réel est désactivé au moment de l'infection ou si la base des signatures de virus n'est plus à jour.

Nous recommandons d'exécuter une analyse d'ordinateur à la demande au moins une fois par mois. L'analyse peut être configurée comme tâche planifiée dans **Outils** > **Planificateur**.

4.2.1.4.1 Type d'analyse

Deux types d'analyses de l'ordinateur à la demande sont disponibles. L'**analyse intelligente** analyse le système sans exiger de reconfiguration des paramètres d'analyse. L'**analyse personnalisée** permet de sélectionner l'un des profils d'analyse prédéfinis, ainsi que de choisir des cibles spécifiques à analyser.



4.2.1.4.1.1 Analyse intelligente

L'analyse intelligente permet de lancer rapidement une analyse de l'ordinateur et de nettoyer les fichiers infectés sans intervention de l'utilisateur. Elle présente l'avantage d'être facile à utiliser, sans aucune configuration d'analyse détaillée. L'analyse intelligente vérifie tous les fichiers des disques locaux, et nettoie ou supprime automatiquement les infiltrations détectées. Le niveau de nettoyage est automatiquement réglé sur sa valeur par défaut. Pour plus d'informations sur les types de nettoyage, reportez-vous à la section Nettoyage.

4.2.1.4.1.2 Analyse personnalisée

L'analyse personnalisée est une solution optimale si vous souhaitez spécifier des paramètres d'analyse tels que les cibles et les méthodes d'analyse. L'analyse personnalisée a l'avantage de permettre la configuration précise des paramètres. Les configurations peuvent être enregistrées sous forme de profils d'analyse définis par l'utilisateur, utiles pour effectuer régulièrement une analyse avec les mêmes paramètres.

Pour sélectionner des cibles à analyser, sélectionnez **Analyse de l'ordinateur** > **Analyse personnalisée**, puis sélectionnez une option dans le menu déroulant **Cibles à analyser** ou sélectionnez des cibles spécifiques dans l'arborescence. Une cible d'analyse peut aussi être spécifiée plus précisément : vous devez indiquer le chemin d'accès au dossier ou aux fichiers à inclure. Si vous souhaitez uniquement effectuer une analyse du système sans ajouter d'actions de nettoyage supplémentaires, sélectionnez l'option **Analyse sans nettoyage**. Vous pouvez aussi choisir parmi trois niveaux de nettoyage en cliquant sur **Configuration...** > **Nettoyage**.

4.2.1.4.2 Cibles à analyser

Le menu déroulant des cibles à analyser permet de sélectionner les fichiers, dossiers et périphériques (disques) à soumettre à l'analyse antivirus.

Par paramètres de profil : permet de sélectionner les cibles indiquées dans le profil d'analyse sélectionné.

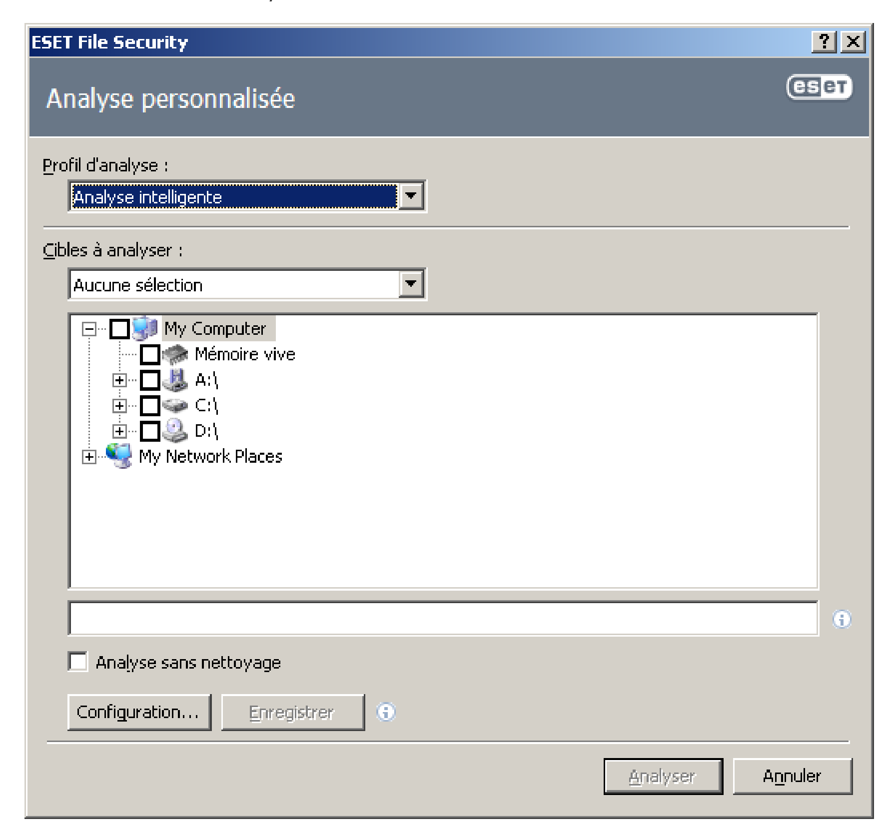
Supports amovibles : permet de sélectionner les disquettes, les périphériques USB, les CD/DVD, etc.

Disques locaux : permet de sélectionner tous les disques durs système.

Disques réseau : permet de sélectionner tous les lecteurs mappés.

Aucune sélection : annule toutes les sélections.

Vous pouvez également définir plus précisément une cible d'analyse en entrant le chemin du dossier ou des fichiers à inclure dans l'analyse. Sélectionnez les cibles dans l'arborescence des périphériques disponibles sur l'ordinateur.

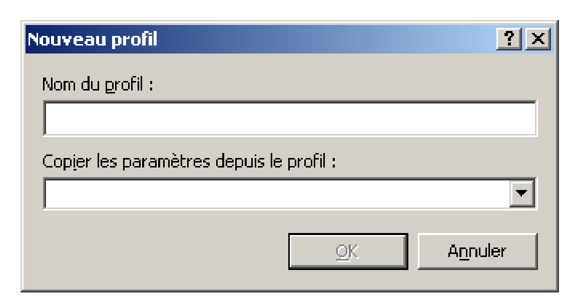


4.2.1.4.3 Profils d'analyse

Vos paramètres d'analyse préférés peuvent être enregistrés pour les prochaines analyses. Il est recommandé de créer autant de profils (avec différentes cibles et méthodes, et d'autres paramètres d'analyse) que d'analyses utilisées régulièrement.

Pour créer un nouveau profil, ouvrez la fenêtre Configuration avancée (F5) et cliquez sur **Analyse de l'ordinateur à la demande** > **Profils...** La fenêtre **Profils de configuration** dispose d'un menu déroulant répertoriant les profils d'analyse existants, ainsi qu'une option permettant de créer un profil. Pour plus d'informations sur la création d'un profil d'analyse, reportez-vous à la section Configuration du moteur ThreatSense ; vous y trouverez la description de chaque paramètre de configuration de l'analyse.

EXEMPLE : Supposons la situation suivante : vous souhaitez créer votre propre profil d'analyse et la configuration d'analyse intelligente est partiellement adéquate. En revanche, vous ne souhaitez analyser ni les fichiers exécutables compressés par un compresseur d'exécutables, ni les applications potentiellement dangereuses. Vous souhaitez effectuer un **nettoyage strict**. Dans la fenêtre **Profils de configuration**, cliquez sur le bouton **Ajouter...** Saisissez le nom de votre nouveau profil dans le champ **Nom du profil** et sélectionnez **Analyse intelligente** dans le menu déroulant **Copier les paramètres depuis le profil** : . Adaptez ensuite les autres paramètres à vos besoins.



4.2.1.4.4 Ligne de commande

Le module antivirus d'ESET File Security peut être lancé depuis la ligne de commande, manuellement (avec la commande « ecls ») ou au moyen d'un fichier de traitement par lots (« bat »).

Les paramètres suivants peuvent être utilisés lors de l'exécution de l'analyseur à la demande à partir de la ligne de commande :

Options générales :

- help	afficher l'aide et quitter
- version	afficher les informations de version et quitter
- base-dir = FOLDER	charger les modules depuis le DOSSIER
- quar-dir = FOLDER	DOSSIER de quarantaine
- aind	afficher l'indicateur d'activité

Cibles :

- files	analyser les fichiers (valeur par défaut)
- no-files	ne pas analyser les fichiers
- boots	analyser les secteurs d'amorçage (valeur par défaut)
- no-boots	ne pas analyser les secteurs d'amorçage
- arch	analyser les archives (valeur par défaut)
- no-arch	ne pas analyser les archives
- max-archive-level = LEVEL	niveau (LEVEL) d'imbrication maximum d'archives
- scan-timeout = LIMIT	analyser les archives pendant un maximum de LIMIT (LIMITE) secondes. Si la durée d'analyse atteint cette limite, l'analyse de l'archive s'arrête et reprend au fichier

	suivant.
- max-arch-size=SIZE	analyser uniquement les SIZE (TAILLE) premiers octets des archives (valeur par défaut 0 = illimité)
- mail	analyser les fichiers de courriers électroniques
- no-mail	ne pas analyser les fichiers des courriers électroniques
- sfx	analyser les archives auto-extractibles
- no-sfx	ne pas analyser les archives auto-extractibles
- rtp	analyser les fichiers exécutables compressés
- no-rtp	ne pas analyser les fichiers exécutables compressés
- exclude = FOLDER	exclure de l'analyse le dossier FOLDER
- subdir	analyser les sous-dossiers (valeur par défaut)
- no-subdir	ne pas analyser les sous-dossiers
- max-subdir-level = LEVEL	Niveau (LEVEL) d'imbrication maximum de sous-dossiers (valeur par défaut 0 - illimité)
- symlink	suivre les liens symboliques (valeur par défaut)
- no-symlink	ignorer les liens symboliques
- ext-remove = EXTENSIONS	
- ext-exclude = EXTENSIONS	exclure de l'analyse les EXTENSIONS délimitées par deux-points

Méthodes :

- adware	rechercher les adware/spyware/riskware
- no-adware	ne pas rechercher les adware/spyware/riskware
- unsafe	rechercher les applications potentiellement dangereuses
- no-unsafe	ne pas rechercher les applications potentiellement dangereuses
- unwanted	rechercher les applications potentiellement indésirables
- no-unwanted	ne pas rechercher les applications potentiellement indésirables
- pattern	utiliser les signatures
- no-pattern	ne pas utiliser les signatures
- heur	activer l'heuristique
- no-heur	désactiver l'heuristique
- adv-heur	activer l'heuristique avancée
- no-adv-heur	désactiver l'heuristique avancée

Nettoyage :

- action = ACTION	appliquer l'ACTION aux objets infectés. Actions disponibles : none (aucune), clean (nettoyer), prompt (demander)
- quarantine	copier les fichiers infectés en quarantaine (complète ACTION)

- no-quarantine	ne pas copier les fichiers infectés vers Quarantaine

Journaux :

- log-file=FILE	journaliser les résultats dans un fichier (FICHIER)
- log-rewrite	écraser le fichier de résultats (valeur par défaut - ajouter)
- log-all	également journaliser les fichiers nettoyés
- no-log-all	ne pas journaliser les fichiers nettoyés (valeur par défaut)

Différents codes sortie d'analyse :

0	- aucune menace détectée
1	- menace détectée mais pas nettoyée
10	- certains fichiers infectés restants
101	- erreur d'archive
102	- erreur d'accès
103	- erreur interne

REMARQUE : un code sortie supérieur à 100 signale un fichier non analysé qui est potentiellement infecté.

4.2.1.5 Performances

Dans cette section, vous pouvez définir le nombre de moteurs d'analyse ThreatSense qui doivent être utilisés pour l'analyse de virus. Un nombre supérieur de moteurs d'analyse ThreatSense sur des ordinateurs multiprocesseurs peut augmenter la vitesse de l'analyse. Une valeur acceptable est comprise entre 1 et 20.

En l'absence d'autres restrictions, nous recommandons d'augmenter le nombre de moteurs d'analyse ThreatSense dans la fenêtre Paramères avancés (F5) sous **Protection de l'ordinateur** > **Antivirus et antispyware** > **Performances**, en respectant la formule suivante : *nombre de moteurs d'analyse ThreatSense = (nombre de processeurs physiques x 2) + 1*. Voici un exemple :

Imaginons que votre serveur comporte 4 unités centrales physiques. Pour des performances optimales, conformément à la formule qui précède, vous devez avoir 9 moteurs d'analyse.

REMARQUE : les modifications apportées ici sont appliquées uniquement après le redémarrage.

4.2.1.6 Filtrage des protocoles

La protection antivirus des protocoles d'application POP3 et HTTP est fournie par le moteur d'analyse ThreatSense qui intègre en toute transparence toutes les techniques avancées d'analyse des logiciels malveillants. Le contrôle fonctionne automatiquement, indépendamment du navigateur Internet ou du client de messagerie utilisés. Les options suivantes sont disponibles pour le filtrage des protocoles (si l'option **Activer le filtrage du contenu des protocoles d'application** est sélectionnée) :

Ports HTTP et POP3 : limite l'analyse de la communication aux ports HTTP et POP3 connus.

Applications marquées comme navigateurs Internet et clients de messagerie : activez cette option pour ne filtrer la communication que des applications marquées comme navigateurs (**Protection de l'accès Web** > **HTTP, HTTPS** > **Navigateurs Web**) et clients de messagerie (**Protection du client de messagerie** > **POP3, POP3s** > **Clients de messagerie**).

Ports et applications marqués comme navigateurs Internet ou clients de messagerie : les ports et les navigateurs font l'objet de recherches de logiciels malveillants.

REMARQUE : à partir de Windows Vista Service Pack 1 et de Windows Server 2008, une nouvelle méthode de filtrage des communications est utilisée. Par conséquent, la section relative au filtrage des protocoles n'est plus disponible.

4.2.1.6.1 SSL

ESET File Security vous permet de vérifier les protocoles encapsulés dans le protocole SSL. Vous pouvez utiliser plusieurs modes d'analyse pour les communications SSL protégées à l'aide de certificats approuvés, de certificats inconnus ou de certificats exclus de la vérification des communications SSL protégées.

Toujours analyser le protocole SSL : sélectionnez cette option pour analyser toutes les communications SSL protégées, à l'exception des communications protégées par des certificats exclus de la vérification. Si une nouvelle communication utilisant un certificat signé inconnu est établie, vous n'êtes pas informé et la communication est automatiquement filtrée. Lorsque vous accéder à un serveur disposant d'un certificat non approuvé et que vous marquez comme approuvé (il est ajouté à la liste des certificats approuvés), la communication vers le serveur est autorisée et le contenu du canal de communication est filtré.

Demander pour les sites non visités (des exclusions peuvent être définies) : si vous accédez à un nouveau site protégé par SSL (dont le certificat est inconnu), vous êtes invité à confirmer que vous souhaitez le visiter avant d'être autorisé à le faire. Ce mode vous permet de créer la liste des certificats SSL qui seront exclus de l'analyse.

Ne pas analyser le protocole SSL : si cette option est activée, le programme n'analyse pas les communications SSL.

S'il est impossible de vérifier le certificat à l'aide du TRCA (**Filtrage des protocoles** > **SSL** > **Certificats**) :

Interroger sur la validité de la certification : invite l'utilisateur à choisir une action à exécuter.

Bloquer toute communication utilisant le certificat : met fin à la connexion au site utilisant le certificat.

Si le certificat est non valide ou endommagé (**Filtrage de protocole** > **SSL** > **Certificats**) :

Interroger sur la validité de la certification : invite l'utilisateur à choisir une action à exécuter.

Bloquer toute communication utilisant le certificat : met fin à la connexion au site utilisant le certificat.

4.2.1.6.1.1 Certificats approuvés

Outre le magasin TRCA intégré dans lequel ESET File Security stocke les certificats approuvés, vous pouvez créer une liste personnalisée de certificats approuvés qui est disponible dans **Configuration avancée** (F5) > **Filtrage des protocoles** > **SSL** > **Certificats** > **Certificats approuvés**.

4.2.1.6.1.2 Certificats exclus

La section Certificats exclus contient des certificats considérés comme étant sûrs. Le contenu des communications chiffrées qui utilisent les certificats répertoriés dans la liste des certificats exclus ne fait pas l'objet de recherche de menaces. Il est recommandé de n'exclure que les certificats Web qui sont garantis comme étant sécurisés et dont la communication utilisant les certificats n'a pas besoin d'être vérifiée.

4.2.1.7 Configuration des paramètres du moteur ThreatSense

ThreatSense est une technologie qui comprend des méthodes de détection de menaces complexes. C'est une technologie proactive : elle fournit une protection dès les premières heures de propagation d'une nouvelle menace. Elle utilise une combinaison de plusieurs méthodes (analyse de code, émulation de code, signatures génériques, signatures de virus) qui se conjuguent pour améliorer sensiblement la sécurité du système. Ce moteur d'analyse est capable de contrôler plusieurs flux de données simultanément, ce qui maximise l'efficacité et le taux de détection. La technologie ThreatSense élimine avec succès les rootkits.

Les options de configuration de la technologie ThreatSense permettent de spécifier plusieurs paramètres d'analyse :

- les types de fichiers et les extensions à analyser ;
- la combinaison de plusieurs méthodes de détection ;
- les niveaux de nettoyage, etc.

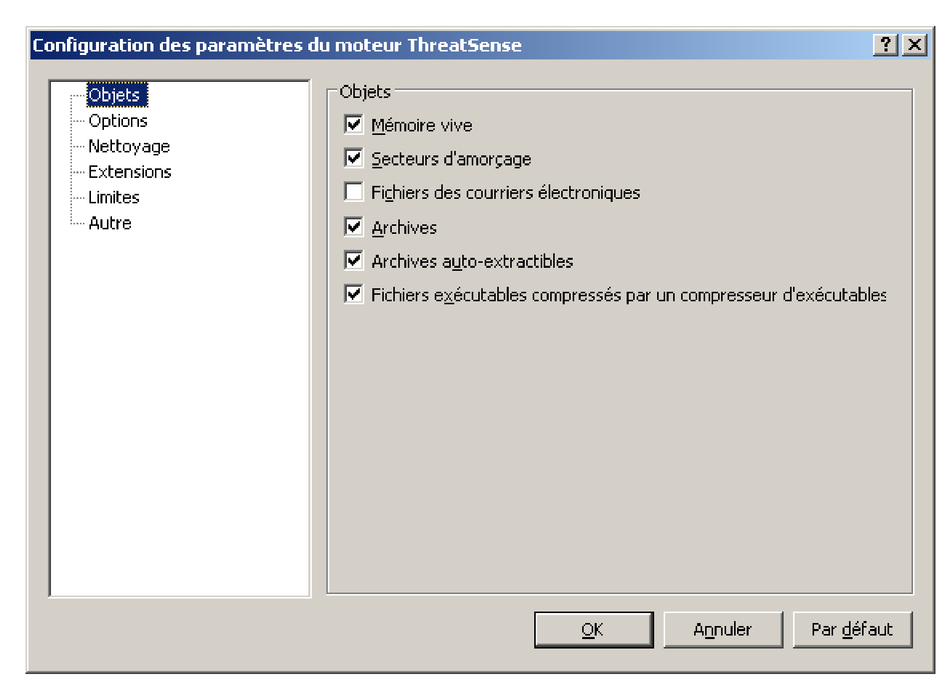
Pour ouvrir la fenêtre de configuration, cliquez sur le bouton **Configuration...** situé dans la fenêtre de configuration de tous les modules qui utilisent la technologie ThreatSense (reportez-vous aux informations ci-dessous). Chaque scénario de sécurité peut exiger une configuration différente. ThreatSense est configurable individuellement pour les modules de protection suivants :

- Protection en temps réel du système de fichiers
- Contrôle des fichiers de démarrage du système
- Protection de la messagerie
- Protection de l'accès Web
- Analyse de l'ordinateur à la demande

Les paramètres ThreatSense sont spécifiquement optimisés pour chaque module et leur modification peut avoir une incidence significative sur le fonctionnement du système. Par exemple, en modifiant les paramètres pour toujours analyser les fichiers exécutables compressés par un compresseur d'exécutables ou pour autoriser l'heuristique avancée dans le module de protection en temps réel du système de fichiers, vous pouvez dégrader les performances du système (normalement, seuls les nouveaux fichiers sont analysés par ces méthodes). Il est donc recommandé de ne pas modifier les paramètres par défaut de ThreatSense pour tous les modules, à l'exception du module d'analyse à la demande de l'ordinateur.

4.2.1.7.1 Configuration des objets

La section **Objets** permet de définir les fichiers et les composants de l'ordinateur qui vont faire l'objet d'une analyse visant à rechercher les éventuelles infiltrations.



Mémoire vive : lance une analyse visant à rechercher les menaces qui attaquent la mémoire vive du système.

Secteurs d'amorçage : analyse les secteurs d'amorçage afin de détection la présence éventuelle de virus dans l'enregistrement d'amorçage principal.

Fichiers : analyse tous les types de fichiers courants (programmes, images, musiques, vidéos, bases de données, etc.).

Fichiers des courriers électroniques : analyse les fichiers spéciaux contenant des messages électroniques.

Archives : analyse les fichiers compressés dans les archives (.rar, .zip, .arj, .tar, etc.).

Archives auto-extractibles : analyse les fichiers contenus dans les archives auto-extractibles et portant généralement l'extension .exe.

Fichiers exécutables compressés par un compresseur d'exécutables : contrairement aux types d'archives standard, les fichiers exécutables compressés par un compresseur d'exécutables sont décompressés en mémoire, en plus des fichiers exécutables compressés statiques standard (UPX, yoda, ASPack, FGS, etc.).

REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le

même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.2.1.7.2 Options

Vous pouvez sélectionner dans la section **Options** les méthodes à utiliser lors de la recherche d'infiltrations dans le système. Les options disponibles sont les suivantes :

Signatures : les signatures permettent de détecter et d'identifier de manière précise et fiable toutes les infiltrations par leur nom grâce aux signatures de virus.

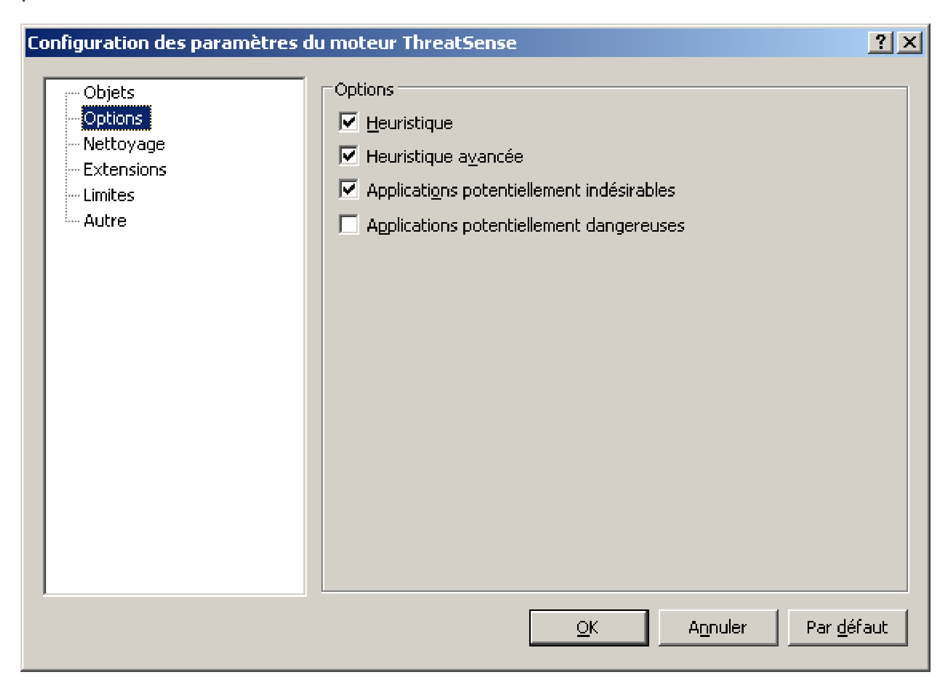
Heuristique : l'heuristique est un algorithme qui analyse l'activité (malveillante) des programmes. La détection heuristique présente l'avantage de détecter les nouveaux logiciels malveillants qui n'existaient pas auparavant ou qui ne figurent pas dans la liste des virus connus (base des signatures de virus).

Heuristique avancée : cette option utilise un algorithme heuristique unique développé par ESET et optimisé pour la détection de vers informatiques et de chevaux de Troie écrits dans des langages de programmation de haut niveau. Grâce à l'heuristique avancée, les capacités de détection du programme sont très élevées.

Logiciels espions/publicitaires/à risque : cette catégorie comprend les logiciels qui collectent diverses informations confidentielles sur les utilisateurs sans leur consentement. Elle inclut également les logiciels qui affichent des publicités.

Détection des applications potentiellement indésirables : les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais peuvent avoir une incidence négative sur les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Les changements les plus significatifs concernent l'affichage indésirable de fenêtres contextuelles, l'activation et l'exécution de processus cachés, l'augmentation de l'utilisation des ressources système, les changements dans les résultats de recherche et les applications communiquant avec des serveurs distants.

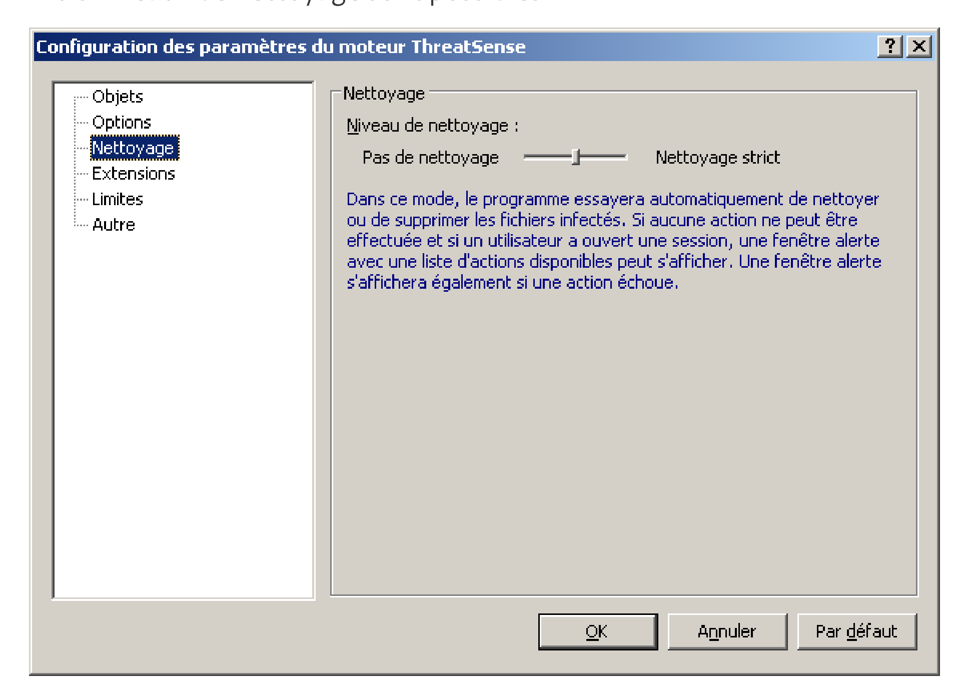
Applications potentiellement dangereuses : cette classification couvre les logiciels commerciaux légitimes. Elle inclut des programmes tels que des outils d'accès à distance. C'est pour cette raison que cette option est désactivée par défaut.



REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.2.1.7.3 Nettoyage

Les paramètres de nettoyage déterminent le comportement de l'analyseur lors du nettoyage des fichiers infectés. Trois niveaux de nettoyage sont possibles :



Pas de nettoyage : les fichiers infectés ne sont pas nettoyés automatiquement. Le programme affiche une fenêtre d'avertissement et permet à l'utilisateur de choisir une action.

Nettoyage standard : le programme essaie de nettoyer ou de supprimer automatiquement tout fichier infecté. S'il n'est pas possible de sélectionner automatiquement l'action correcte, le programme propose différentes actions de suivi. Cette sélection s'affiche également si une action prédéfinie ne peut pas être menée à bien.

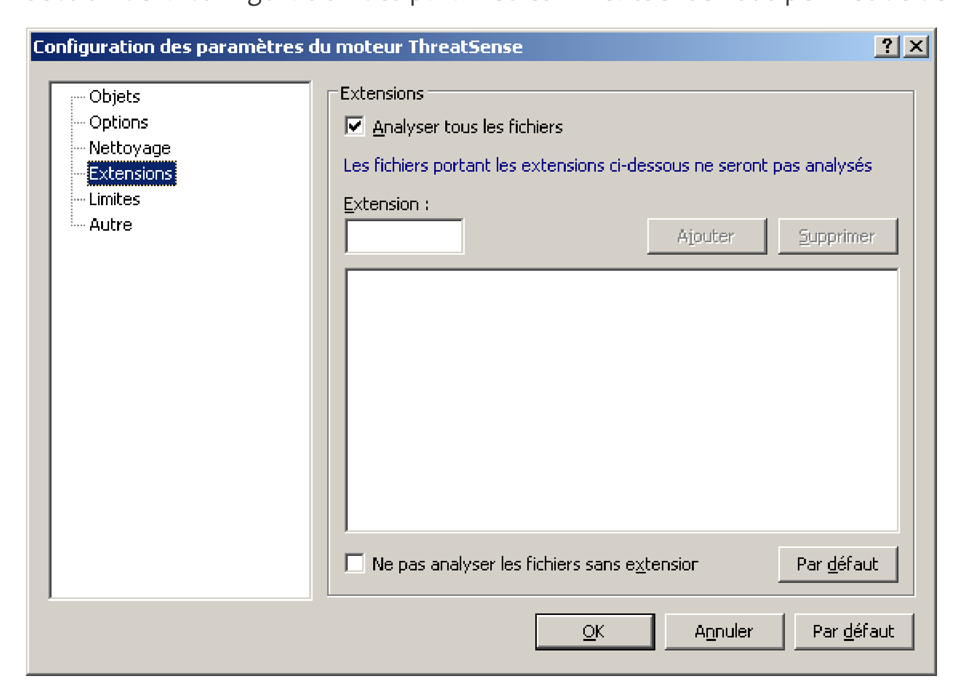
Nettoyage strict : le programme nettoie ou supprime tous les fichiers infectés (y compris les archives). Les seules exceptions sont les fichiers système. S'il n'est pas possible de les nettoyer, la fenêtre d'avertissement qui s'affiche propose différentes options.

Avertissement : Dans le mode par défaut, le fichier d'archive n'est entièrement supprimé que si tous les fichiers qu'il contient sont infectés. Si l'archive contient également des fichiers légitimes, elle n'est pas supprimée. Si un fichier d'archive infecté est détecté dans le mode Nettoyage strict, le fichier entier est supprimé, même s'il contient également des fichiers intacts.

REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.2.1.7.4 Extensions

L'extension est la partie du nom de fichier située après le point. Elle définit le type et le contenu du fichier. Cette section de la configuration des paramètres ThreatSense vous permet de définir les types de fichiers à analyser.



Par défaut, tous les fichiers sont analysés, quelle que soit leur extension. Toutes les extensions peuvent être ajoutées à la liste des fichiers exclus de l'analyse. Si l'option **Analyser tous les fichiers** est désélectionnée, la liste change et affiche toutes les extensions des fichiers analysés. Les boutons **Ajouter** et **Supprimer** permettent d'activer ou d'empêcher l'analyse des extensions souhaitées.

Pour activer l'analyse de fichiers sans extension, sélectionnez l'option **Analyser les fichiers sans extension**.

L'exclusion de fichiers de l'analyse peut être utile si l'analyse de certains types de fichiers provoque un dysfonctionnement du programme utilisant ces extensions. Par exemple, il peut être judicieux d'exclure les extensions .edb, .eml et .tmp si vous utilisez le serveur Microsoft Exchange.

REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.2.1.7.5 Limites

La section Limites permet de spécifier la taille maximale des objets et les niveaux d'imbrication des archives à analyser :

Taille d'objet maximale : définit la taille maximum des objets à analyser. Le module antivirus n'analyse alors que des objets d'une taille inférieure à celle spécifiée. Il n'est pas recommandé de modifier la valeur par défaut et il n'y a généralement aucune raison de le faire. Cette option ne doit être modifiée que par des utilisateurs chevronnés ayant des raisons très précises d'exclure de l'analyse les objets plus volumineux.

Durée d'analyse maximale pour l'objet (s) : définit la durée maximum attribuée à l'analyse d'un objet. Si la valeur de ce champ a été définie par l'utilisateur, le module antivirus cesse d'analyser un objet une fois ce temps écoulé, que l'analyse soit terminée ou non.

Niveau d'imbrication des archives : indique le nombre maximal de niveaux analysés dans les archives. Il n'est pas recommandé de modifier la valeur par défaut (10). Dans des circonstances normales, il n'y a aucune raison de le faire. Si l'analyse prend fin prématurément en raison du nombre d'archives imbriquées, l'archive reste non vérifiée.

Taille maximale de fichier dans l'archive : cette option permet de spécifier la taille maximale (après extraction) des fichiers à analyser qui sont contenus dans les archives. Si l'analyse d'une archive prend fin prématurément pour cette raison, l'archive reste non vérifiée.

REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.2.1.7.6 Autre

Analyser les flux de données alternatifs (ADS) : les flux de données alternatifs (ADS) utilisés par le système de fichiers NTFS sont des associations de fichiers et de dossiers que les techniques d'analyse ordinaires ne permettent pas de détecter. De nombreuses infiltrations tentent d'éviter la détection en se faisant passer pour des flux de données alternatifs.

Exécuter les analyses en arrière-plan avec une priorité faible : toute séquence d'analyse consomme une certaine quantité de ressources système. Si vous utilisez des programmes qui exigent beaucoup de ressources système, vous pouvez activer l'analyse en arrière-plan à faible priorité de manière à réserver des ressources pour vos applications.

Journaliser tous les objets : si cette option est sélectionnée, le fichier journal affiche tous les fichiers analysés, même ceux qui ne sont pas infectés.

Activer l'optimalisation intelligente : sélectionnez cette option pour que les fichiers déjà analysés ne soient pas analysés plusieurs fois (sauf s'ils ont été modifiés). Les fichiers sont immédiatement réanalysés après chaque mise à jour de la base des signatures de virus.

Conserver la date et l'heure du dernier accès : sélectionnez cette option pour conserver l'heure d'accès d'origine des fichiers analysés au lieu de la mettre à jour (par exemple pour l'utiliser avec des systèmes de sauvegarde de données).

Dérouler journal : cette option permet d'autoriser/interdire le défilement du journal. Si cette option est sélectionnée, les informations défilent vers le haut dans la fenêtre d'affichage.

Afficher la notification de fin d'analyse dans une fenêtre séparée : ouvre une fenêtre indépendante contenant des informations sur les résultats d'analyse.

REMARQUE: Lorsqu'un point bleu s'affiche en regard d'un paramètre, cela indique que son réglage diffère de celui défini pour d'autres modules qui utilisent également ThreatSense. Étant donné que vous pouvez configurer le même paramètre différemment pour chaque module, ce point bleu n'est qu'un simple rappel que ce même paramètre est configuré différemment pour d'autres modules. L'absence de point bleu signifie que le paramètre de tous les modules est configuré de la même manière.

4.2.1.8 Une infiltration est détectée

Des infiltrations peuvent atteindre le système à partir de différents points d'entrée : pages Web, dossiers partagés, courrier électronique ou périphériques amovibles (USB, disques externes, CD, DVD, disquettes, etc.).

Si votre ordinateur montre des signes d'infection par un logiciel malveillant (ralentissement, blocages fréquents, etc.), nous recommandons d'effectuer les opérations suivantes :

- Ouvrez ESET File Security et cliquez sur Analyse de l'ordinateur.
- Cliquez sur **Analyse intelligente** (pour plus d'informations, reportez-vous à la section Analyse intelligente).
- Lorsque l'analyse est terminée, consultez le journal pour connaître le nombre de fichiers analysés, infectés et nettoyés.

Si vous ne souhaitez analyser qu'une certaine partie de votre disque, cliquez sur **Analyse personnalisée** et sélectionnez des cibles à analyser.

Pour donner un exemple général de la façon dont les infiltrations sont traitées dans ESET File Security, supposons qu'une infiltration soit détectée par la protection en temps réel du système de fichiers, qui utilise le niveau de nettoyage par défaut. Le programme tente de nettoyer ou de supprimer le fichier. Si aucune action n'est prédéfinie pour le module de protection en temps réel, vous êtes invité à sélectionner une option dans une fenêtre d'avertissement. Généralement, les options **Nettoyer**, **Supprimer** et **Aucune action** sont disponibles. Il n'est pas recommandé de sélectionner **Aucune action**, car les fichiers infectés sont conservés tels quels. La seule exception concerne les situations où vous êtes sûr que le fichier est inoffensif et qu'il a été détecté par erreur.

Nettoyage et suppression : utilisez le nettoyage si un fichier sain a été attaqué par un virus qui y a joint du code malveillant. Dans ce cas, essayez d'abord de nettoyer le fichier infecté pour le restaurer dans son état d'origine. Si le

fichier se compose uniquement de code malveillant, il est supprimé.



Si un fichier infecté est « verrouillé » ou utilisé par un processus système, il n'est généralement supprimé qu'après avoir été déverrouillé (normalement, après un redémarrage du système).

Suppression de fichiers dans des archives : en mode de nettoyage par défaut, l'archive complète n'est supprimée que si elle ne contient que des fichiers infectés et aucun fichier sain. Autrement dit, les archives ne sont pas supprimées si elles contiennent également des fichiers sains. Cependant, soyez prudent si vous choisissez un nettoyage strict : dans ce mode, l'archive est supprimée si elle contient au moins un fichier infecté, quel que soit l'état des autres fichiers qu'elle contient.

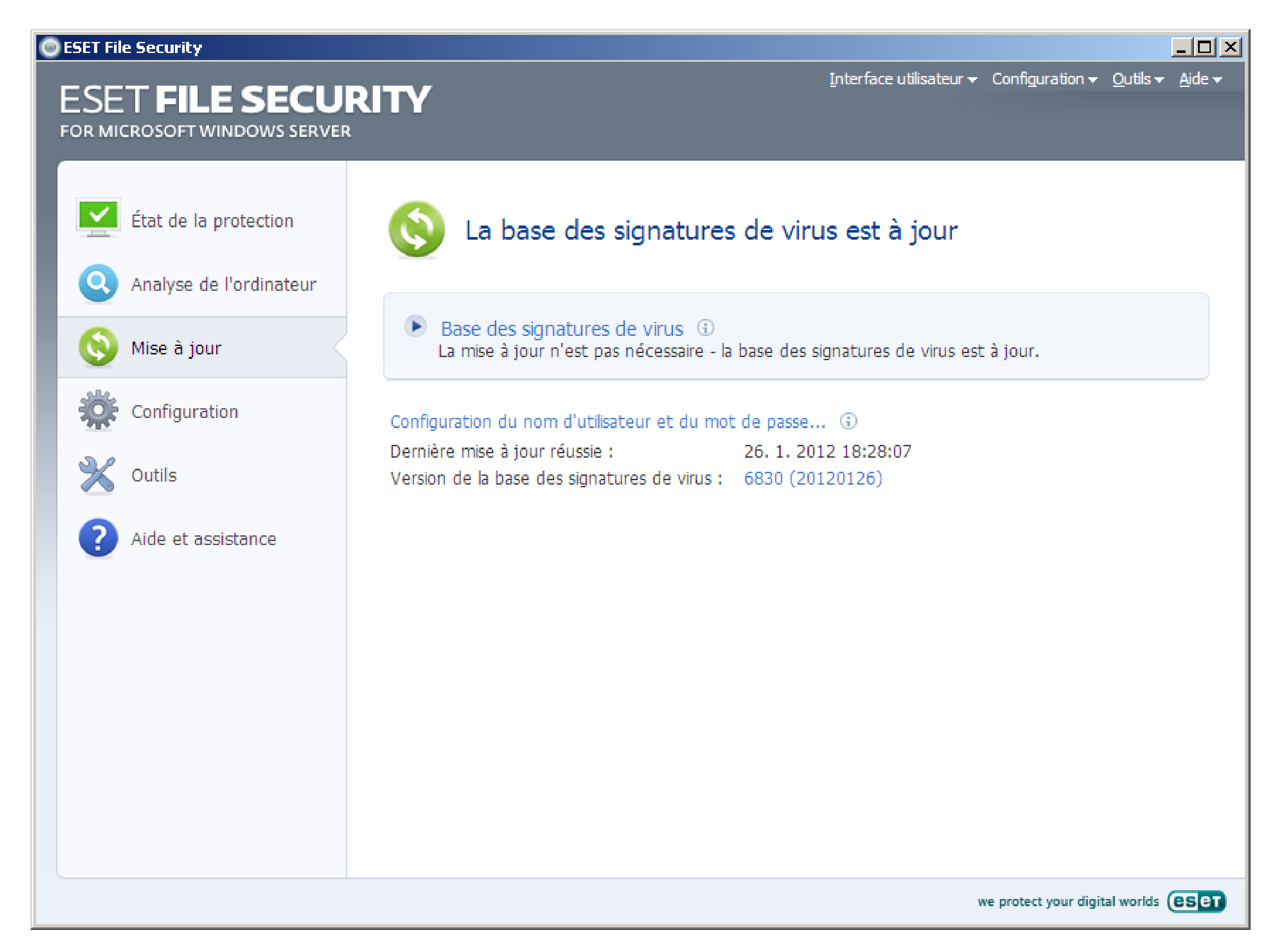
4.3 Mise à jour du programme

La mise à jour régulière d'ESET File Security est la condition de base pour l'obtention du niveau maximum de sécurité. Le module de mise à jour veille à ce que le programme soit toujours à jour de deux façons : en mettant à jour la base des signatures de virus et en mettant à jour les composants système.

En cliquant sur **Mettre à jour** dans le menu principal, vous pouvez connaître l'état actuel de la mise à jour, notamment la date et l'heure de la dernière mise à jour. Vous pouvez également savoir si une mise à jour est nécessaire. La fenêtre Mise à jour contient également la version de la base des signatures de virus. Cette indication numérique est un lien actif vers le site Web d'ESET, qui répertorie toutes les signatures ajoutées dans cette mise à jour.

Par ailleurs, l'option permettant de commencer manuellement le processus de mise à jour, **Mettre à jour la base des signatures de virus**, est disponible, de même que les options de configuration de base de la mise à jour telles que le nom d'utilisateur et le mot de passe permettant d'accéder aux serveurs de mise à jour d'ESET.

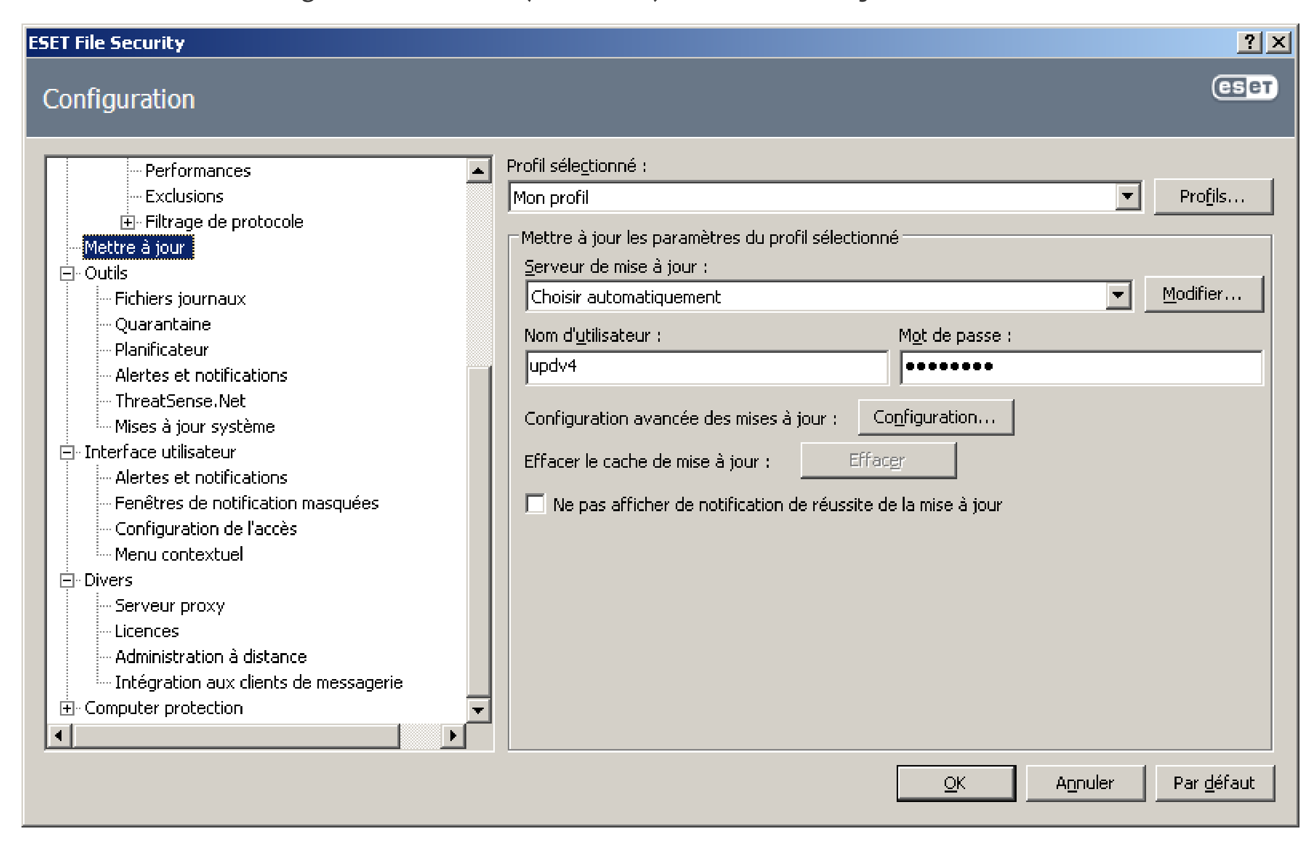
Utilisez le lien **Activation de produit** pour ouvrir un formulaire d'enregistrement qui nous permet d'activer le produit de sécurité ESET et de vous envoyer un courrier électronique avec vos données d'authentification (nom d'utilisateur et mot de passe).



REMARQUE : le nom d'utilisateur et le mot de passe sont fournis par ESET après l'achat d'ESET File Security.

4.3.1 Configuration des mises à jour

La section de la configuration des mises à jour permet de spécifier les informations concernant les sources des mises à jour, telles que les serveurs de mise à jour et les données d'authentification donnant accès à ces serveurs. Par défaut, le menu déroulant **Serveur de mise à jour** est défini sur l'option **Choisir automatiquement**, ce qui garantit que les fichiers de mise à jour sont téléchargés automatiquement depuis le serveur ESET en utilisant le moins de ressources réseau possible. Les options de configuration des mises à jour sont disponibles dans l'arborescence de configuration avancée (touche F5), dans **Mettre à jour**.

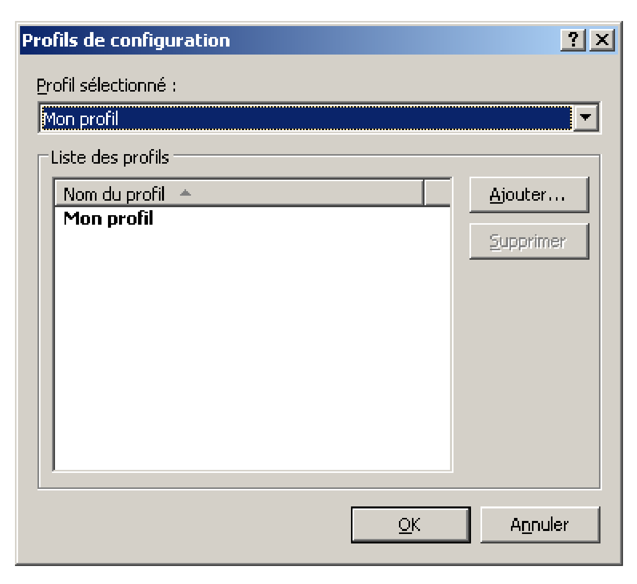


La liste des serveurs de mise à jour disponibles est accessible par l'intermédiaire du menu déroulant **Serveur de mise à jour**. Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier...** dans la section **Mettre à jour les paramètres du profil sélectionné**, puis cliquez sur le bouton **Ajouter**. L'authentification des serveurs de mise à jour est basée sur le **nom d'utilisateur** et le **mot de passe** générés et qui vous ont été envoyés après l'achat.

4.3.1.1 Profils de mise à jour

Les profils de mise à jour ne peuvent pas être créés pour différentes configurations et tâches de mise à jour. La création de profils de mise à jour est particulièrement utile pour les utilisateurs mobiles qui peuvent créer un autre profil correspondant aux propriétés de connexion Internet qui changent régulièrement.

Le menu déroulant **Profil sélectionné** affiche le profil sélectionné ; il est défini par défaut sur **Mon profil**. Pour créer un nouveau profil, cliquez sur les boutons **Profils...** et **Ajouter...**, puis indiquez votre propre **Nom du profil**. Lorsque de la création d'un nouveau profil, vous pouvez copier les paramètres d'un profil existant en le sélectionnant dans le menu déroulant **Copier les paramètres depuis le profil**.



Dans la fenêtre de configuration du profil, vous pouvez indiquer le serveur de mise à jour dans la liste des serveurs disponibles ou encore ajouter un nouveau serveur. La liste des serveurs de mise à jour existants est accessible par l'intermédiaire du menu déroulant **Serveur de mise à jour** : . Pour ajouter un nouveau serveur de mise à jour, cliquez sur **Modifier...** dans la section **Mettre à jour les paramètres du profil sélectionné**, puis cliquez sur le bouton **Ajouter**.

4.3.1.2 Configuration avancée des mises à jour

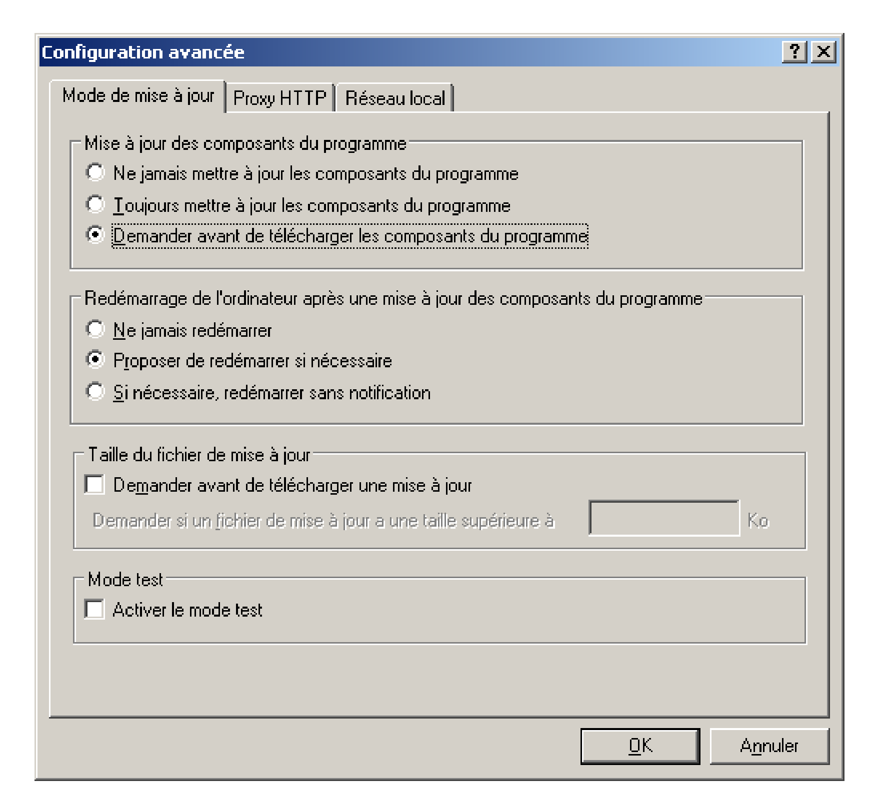
Pour afficher la configuration avancée des mises à jour, cliquez sur le bouton **Configuration...**. Les options de configuration avancée de mise à jour englobent les options **Mode de mise à jour**, **Proxy HTTP**, **Réseau local** et **Miroir**.

4.3.1.2.1 Mode de mise à jour

L'onglet **Mode de mise à jour** contient les options concernant la mise à jour des composants du programme.

Dans la section **Mise à jour des composants du programme**, trois options sont disponibles :

- **Ne jamais mettre à jour les composants du programme** : aucune mise à jour des composants du programme n'est effectuée.
- **Toujours mettre à jour les composants du programme** : Les mises à jour des composants du programme sont effectuées automatiquement.
- **Demander avant de télécharger les composants du programme** : Il s'agit de l'option par défaut. Vous êtes invité à confirmer ou à refuser les mises à jour de composants de programme lorsqu'elles sont disponibles.



Après l'installation d'une mise à jour de composants du programme, il est peut-être nécessaire de redémarrer l'ordinateur afin d'obtenir la pleine fonctionnalité de tous les modules. La section **Redémarrer après une mise à jour des composants du programme** vous permet de choisir l'une des trois options suivantes :

- **Ne jamais redémarrer**
- **Proposer le redémarrage de l'ordinateur si nécessaire**
- **Si nécessaire**, **redémarrer l'ordinateur sans avertissement**

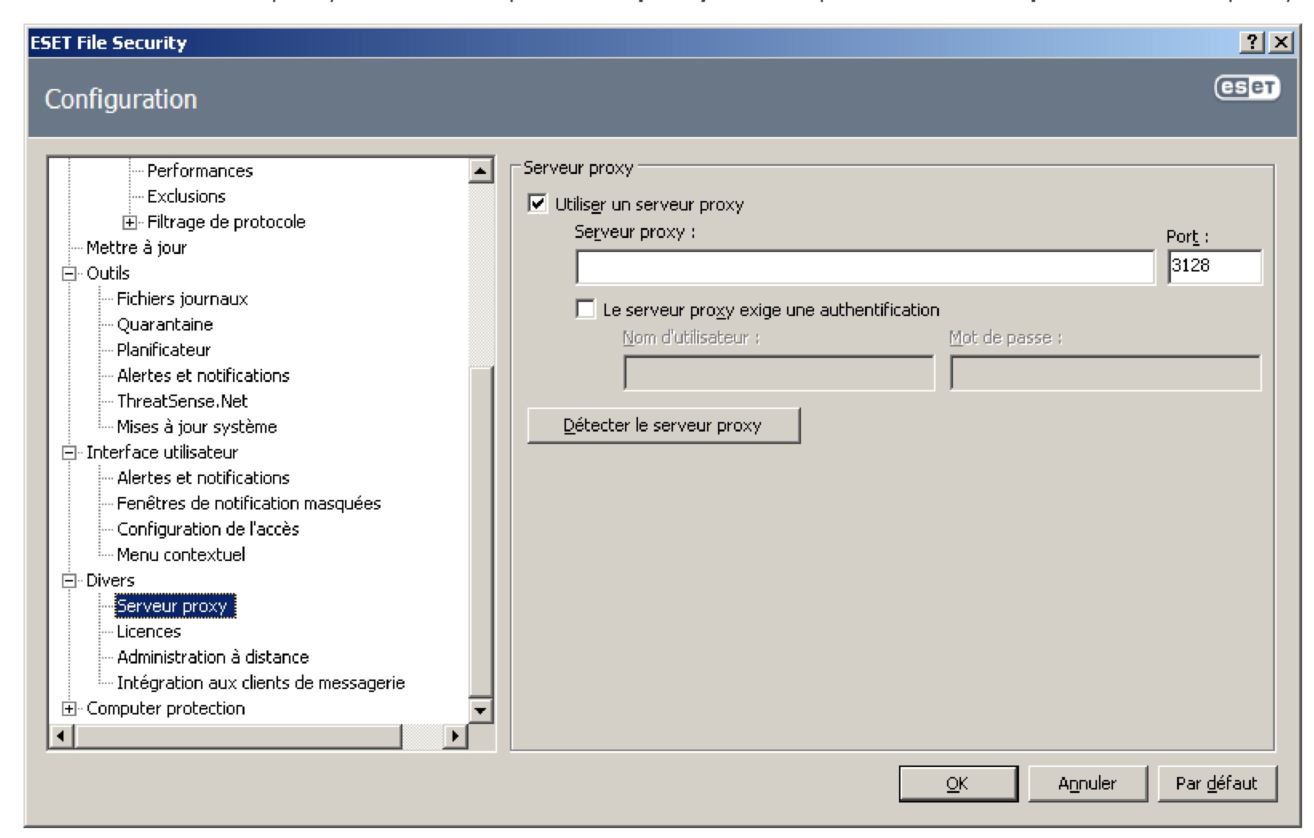
L'option par défaut est **Proposer le redémarrage de l'ordinateur si nécessaire**. La sélection de l'option la plus appropriée dépend du poste de travail sur lequel les paramètres sont appliqués. Notez qu'il existe des différences entre les postes de travail et les serveurs. Par exemple, le redémarrage automatique d'un serveur après une mise à niveau du programme peut causer de sérieux dommages.

4.3.1.2.2 Serveur proxy

Dans ESET File Security, la configuration du serveur proxy est disponible dans deux sections de l'arborescence de configuration avancée.

Les paramètres de serveur proxy peuvent être configurés dans **Divers** > **Serveur proxy**. La spécification du serveur proxy à ce niveau définit les paramètres de serveur proxy globaux pour l'intégralité d'ESET File Security. Les paramètres définis ici seront utilisés par tous les modules exigeant une connexion à Internet.

Pour spécifier des paramètres de serveur proxy à ce niveau, cochez la case **Utiliser un serveur proxy**, puis entrez l'adresse du serveur proxy dans le champ **Serveur proxy** : , ainsi que le numéro de **port** du serveur proxy.



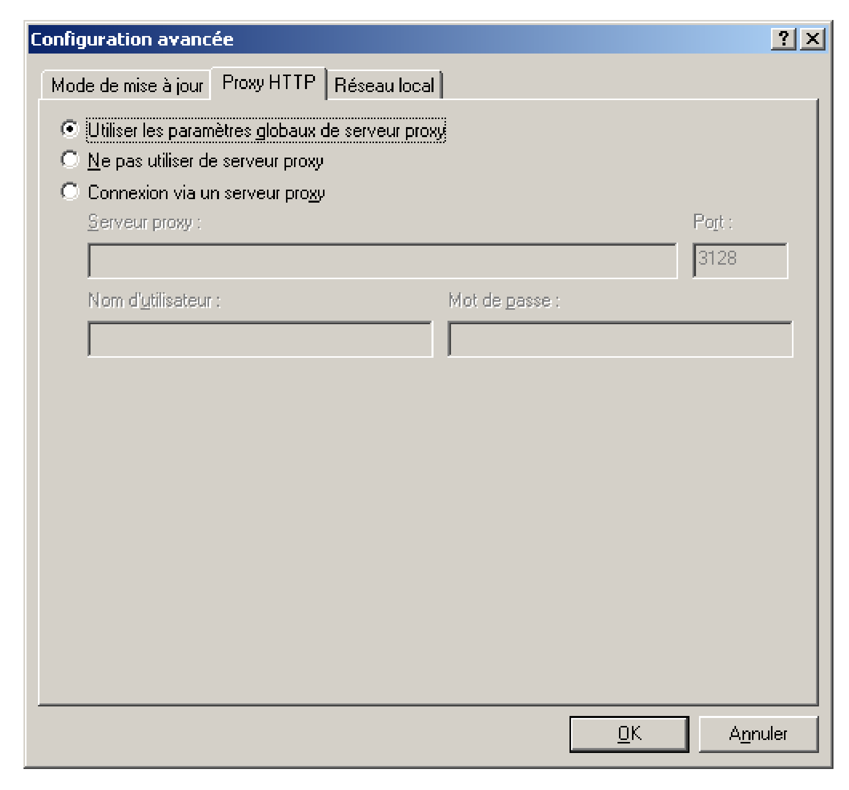
Si la communication avec le serveur proxy exige une authentification, cochez la case **Le serveur proxy nécessite une authentification** et entrez un nom d'utilisateur et un mot de passe valides dans les champs correspondants. Cliquez sur le bouton **Détecter le serveur proxy** pour détecter automatiquement et insérer les paramètres du serveur proxy. Les paramètres indiqués dans Internet Explorer sont copiés.

REMARQUE : cette fonctionnalité ne récupère pas les données d'authentification (nom d'utilisateur et mot de passe) et vous devez les fournir.

Les paramètres de serveur proxy peuvent également être établis dans la configuration avancée de la mise à jour. Ces paramètres s'appliquent au profil de mise à jour donné. Vous pouvez accéder aux options de configuration du serveur proxy pour un profil de mise à jour donné en cliquant sur l'onglet **Proxy HTTP** dans **Configuration avancée des mises à jour**. Vous avez le choix entre ces trois options :

- **Utiliser les paramètres globaux de serveur proxy**
- **Ne pas utiliser de serveur proxy**
- **Connexion via un serveur proxy** (connexion définie par les propriétés de la connexion)

L'option **Utiliser les paramètres globaux de serveur proyx** utilise les options de configuration de serveur proxy déjà indiquées dans la branche **Divers** > **Seveur proxy** de l'arborescence de configuration avancée (comme indiqué précédemment dans le présent article).



Sélectionnez l'option **Ne pas utiliser de serveur proxy** pour indiquer qu'aucun serveur proxy ne sera utilisé pour la mise à jour de ESET File Security.

L'option **Connexion via un serveur proxy** doit être sélectionnée si vous souhaitez utiliser un serveur proxy pour mettre à jour ESET File Security. Ce serveur proxy doit être différent de celui indiqué dans les paramètres globaux (**Divers** > **Serveur proxy**). Si c'est le cas, des paramètres supplémentaires doivent être spécifiés : **l'adresse du serveur** proxy, le **Port** de communication, ainsi que le **Nom d'utilisateur** et le **Mot de passe** du serveur proxy, si nécessaire.

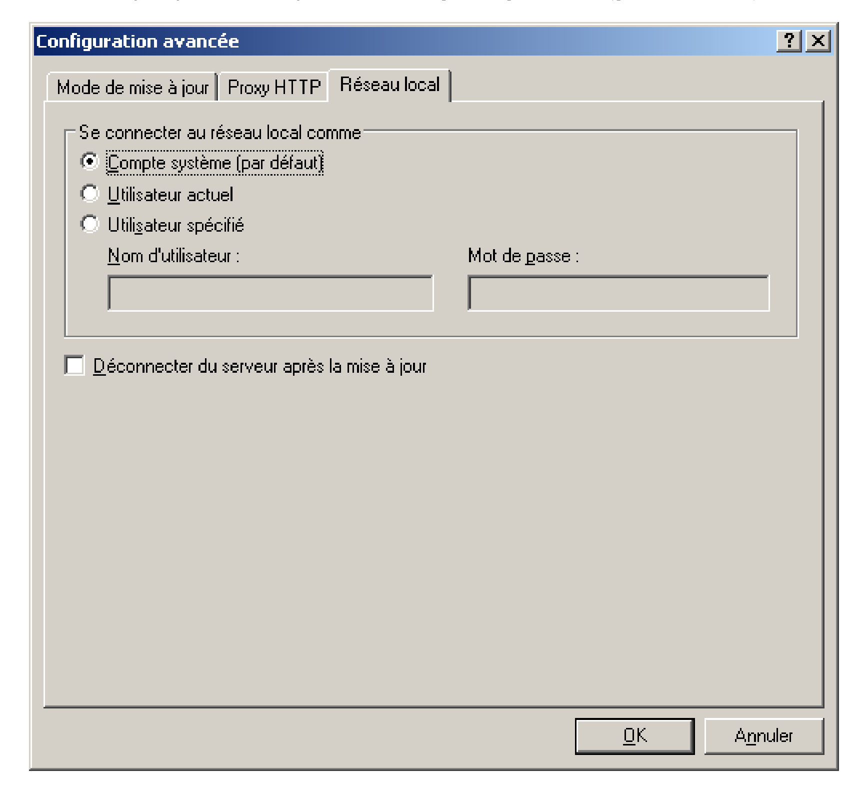
Cette option doit également être sélectionnée si les paramètres de serveur proxy n'ont pas été définis globalement, mais ESET File Security se connecte à un serveur proxy pour les mises à jour.

L'option par défaut pour le serveur proxy est **Utiliser les paramètres globaux de serveur proxy**.

4.3.1.2.3 Connexion au réseau local

Lors de mise à jour depuis un serveur local sur un système d'exploitation NT, une authentification est par défaut exigée pour chaque connexion réseau. Dans la plupart des cas, un compte système local n'a pas suffisamment de droits pour accéder au dossier miroir (ce dossier contient des copies des fichiers de mise à jour). Dans ce cas, entrez un nom d'utilisateur et un mot de passe dans la section de configuration des mises à jour ou spécifiez un compte avec lequel le programme peut accéder au serveur de mise à jour (miroir).

Pour configurer un compte de ce type, cliquez sur l'onglet **Réseau local**. La section **Se connecter au réseau local comme** propose les options **Compte système (par défaut)**, **Utilisateur actuel** et **Utilisateur spécifié**.



Sélectionnez l'option **Compte système (par défaut)** pour utiliser le compte système pour l'authentification. Normalement, aucun traitement d'authentification n'a lieu si des données d'authentification ne sont pas fournies dans la section de configuration des mises à jour.

Pour s'assurer que le programme s'authentifie avec le compte de l'utilisateur actuellement connecté, sélectionnez **Utilisateur actuel**. L'inconvénient de cette solution est que le programme est dans l'impossibilité de se connecter au serveur de mise à jour si aucun utilisateur n'est connecté.

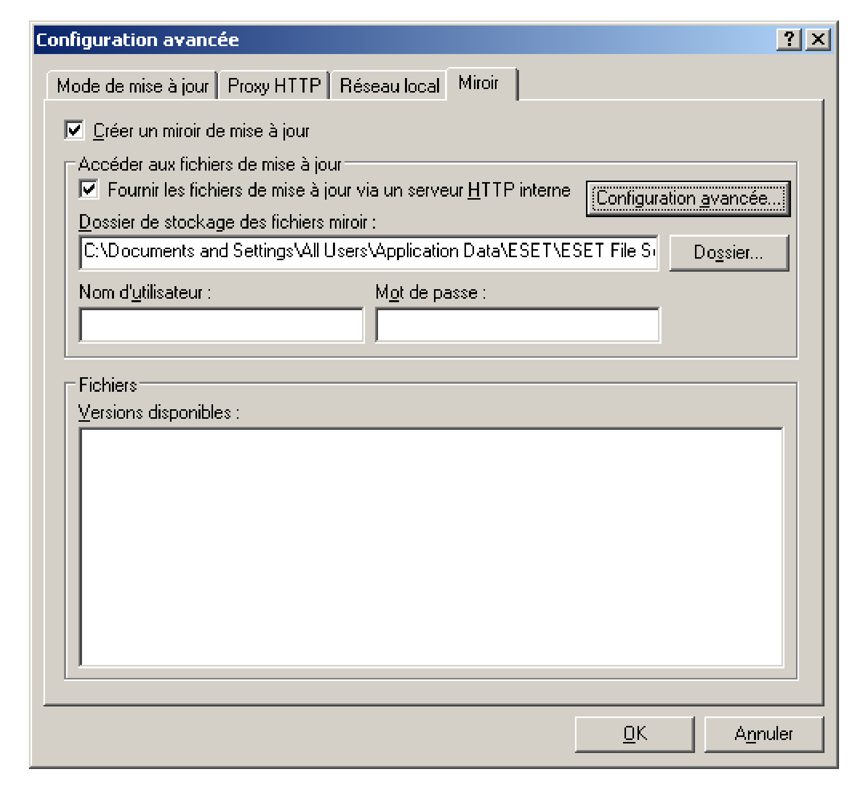
Sélectionnez **Utilisateur spécifié** si vous voulez que le programme utilise un compte utilisateur spécifié pour l'authentification.

Avertissement : Si l'une des options **Utilisateur actuel** ou **Utilisateur spécifié** est sélectionnée, une erreur peut se produire en cas de changement de l'identité du programme pour l'utilisateur souhaité. C'est pour cela que nous recommandons d'entrer les données d'authentification du réseau local dans la section de configuration des mises à jour. Dans cette section de configuration des mises à jour, les données d'authentification doivent être entrées comme suit : nom_de_domaine\utilisateur (dans le cas d'un groupe de travail, entrez nom_de_groupe_de_travail\utilisateur) et le mot de passe de l'utilisateur. La mise à jour de la version HTTP du serveur local n'exige aucune authentification.

4.3.1.2.4 Création de copies de mises à jour : miroir

ESET File Security vous permet de créer des copies des fichiers de mises à jour qui peuvent être utilisées pour la mise à jour d'autres postes de travail du réseau. La mise à jour de postes de travail à partir d'un miroir optimise l'équilibre de la charge réseau et libère les bandes passantes des connexions Internet.

Les options de configuration du serveur miroir local sont accessibles (après l'ajout d'une clé de licence valide dans le gestionnaire de licences dans la section Configuration d'avancée de ESET File Security) dans la section **Configuration avancée des mises à jour** : . Pour accéder à cette section, appuyez sur la touche F5 et cliquez sur **Mettre à jour** dans l'arborescence de configuration avancée, puis cliquez sur le bouton **Configuration...** situé à côté de **Configuration avancée des mises à jour** : , puis sélectionnez l'onglet **Miroir**).



La première étape de configuration du miroir consiste à sélectionner l'option Créer un miroir de mise à jour. La sélection de cette option active d'autres options de configuration du miroir, telles que la manière d'accéder aux fichiers de mise à jour et le chemin des fichiers miroir.

Les méthodes d'activation du miroir sont décrites en détail dans la section Mise à jour à partir du miroir. Pour le moment, notez qu'il existe deux méthodes de base pour accéder au miroir : le dossier des fichiers de mise à jour peut être considéré comme un dossier réseau partagé ou comme un serveur HTTP.

Le dossier dédié aux fichiers de mise à jour du miroir peut être défini dans la section **Dossier de stockage des fichiers miroir**. Cliquez sur **Dossier...** pour naviguer jusqu'au dossier souhaité sur un ordinateur local ou un dossier réseau partagé. Si une autorisation pour le dossier spécifié est requise, les données d'authentification doivent être entrées dans les champs **Nom d'utilisateur** et **Mot de passe**. Le nom d'utilisateur et le mot de passe doivent être entrés sous le format *Domaine/Utilisateur* ou *Workgroup/Utilisateur*. N'oubliez pas de fournir les mots de passe correspondants.

Lors de la configuration du miroir, vous pouvez également spécifier les différentes langues des copies de mises à jour à télécharger. La configuration de la langue de version est accessible dans la section **Fichiers** - **Versions disponibles** :.

4.3.1.2.4.1 Mise à jour à partir du miroir

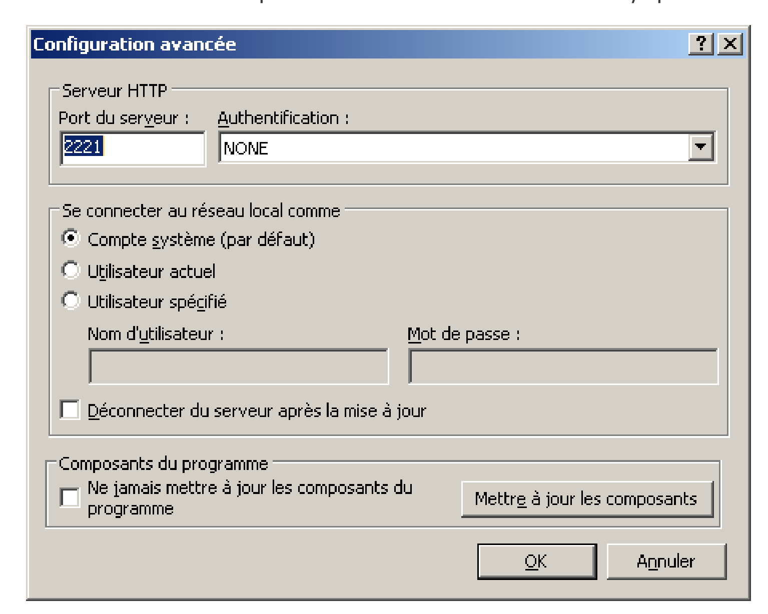
Il existe deux méthodes de base pour configurer le miroir : le dossier des fichiers de mise à jour peut être considéré comme un dossier réseau partagé ou comme un serveur HTTP.

Accès au miroir au moyen d'un serveur HTTP interne

Cette configuration est l'option par défaut ; elle est indiquée dans la configuration du programme prédéfinie. Afin de permettre l'accès au miroir à l'aide du serveur HTTP, accédez aux options **Configuration avancée des mises à jour** (onglet **Miroir**) et sélectionnez l'option **Créer un miroir de mise à jour**.

Dans la section **Configuration avancée** de l'onglet **Miroir**, vous pouvez indiquer le **Port du serveur** sur lequel le serveur HTTP écoute, ainsi que le type d'**Authentification** utilisé par le serveur HTTP. Par défaut, cette option est configurée sur **2221**. L'option **Authentification** définit la méthode d'authentification utilisée pour accéder aux fichiers de mise à jour. Les options disponibles sont les suivantes : **AUCUNE**, **De base** et **NTLM**. Sélectionnez **De base** pour utiliser le codage base64 avec l'authentification de base du nom d'utilisateur et mot de passe. L'option **NTLM** fournit un codage utilisant une méthode de codage fiable. L'utilisateur créé sur le poste de travail partageant les fichiers de mise à jour est utilisé pour l'authentification. L'option par défaut est **AUCUNE**. Elle autorise l'accès aux fichiers des mises à jour sans exiger d'authentification.

Avertissement : l'accès aux fichiers des mises à jour au moyen du serveur HTTP exige que le dossier miroir soit sur le même ordinateur que l'instance ESET File Security qui l'a créé.



Une fois la configuration du miroir terminée, ajoutez aux postes de travail un nouveau serveur de mise à jour dans le format **http://adresse_IP_de_votre_serveur:2221**. Pour ce faire, procédez comme suit :

- Ouvrez **Configuration avancée** de ESET File Security et cliquez sur la branche **Mise à jour**.
- Cliquez sur **Modifier...** à droite du menu contextuel **Serveur de mise à jour** et ajoutez un nouveau serveur en respectant le format suivant : http://IP_adresse_de_votre_serveur:2221.
- Sélectionnez dans la liste des serveurs de mise à jour le serveur nouvellement ajouté.

Accès au miroir via le partage des systèmes

Un dossier partagé doit d'abord être créé sur un lecteur local ou réseau. Lors de la création du dossier pour le miroir, il est nécessaire d'octroyer le droit d'écriture à l'utilisateur qui va sauvegarder les fichiers de mise à jour dans le dossier et le droit de lecture aux utilisateurs qui vont utiliser le dossier miroir pour la mise à jour de ESET File Security.

Continuez ensuite la configuration d'accès au miroir dans la section **Configuration avancée des mises à jour** (onglet **Miroir**) en désactivant l'option **Fournir les fichiers de mise à jour via un serveur HTTP interne**. Cette option est activée par défaut lors de l'installation du programme.

Si le dossier partagé se trouve sur un autre ordinateur du réseau, une authentification est nécessaire pour accéder à l'autre ordinateur. Pour spécifier les données d'authentification, ouvrez Configuration avancée d'ESET File Security (F5) et cliquez sur la branche **Mise à jour**. Cliquez sur le bouton **Configuration...**, puis cliquez sur l'onglet **Réseau**

local. Ce paramètre est le même que celui de la mise à jour, comme l'indique la section Connexion au réseau local.

Une fois la configuration du miroir terminée, continuez avec les postes de travail en spécifiant \\UNC\CHEMIN comme serveur de mise à jour. Cette opération peut s'effectuer comme suit :

- Ouvrez Configuration avancée de ESET File Security et cliquez sur **Mise à jour**
- Cliquez sur **Modifier...** en regard de Serveur de mise à jour et ajoutez un nouveau serveur au *format \\UNC\PATH*.
- Sélectionnez dans la liste des serveurs de mise à jour le serveur nouvellement ajouté.

REMARQUE : pour un fonctionnement correct, le chemin du dossier miroir doit être spécifié comme un chemin UNC. Les mises à jour à partir de lecteurs mappés peuvent ne pas fonctionner.

4.3.1.2.4.2 Dépannage des problèmes de miroir de mise à jour

Dans la plupart des cas, les problèmes de mise à jour depuis un serveur miroir proviennent des raisons suivantes : mauvaise spécification des options du dossier miroir, données d'authentification incorrectes pour l'accès au dossier miroir, mauvaise configuration des postes de travail qui cherchent à télécharger des fichiers de mise à jour du miroir ou combinaison des raisons citées précédemment. Nous donnons ici un aperçu des problèmes les plus fréquents qui peuvent se produire lors d'une mise à jour depuis le miroir :

ESET File Security **signale une erreur de connexion au serveur miroir** : l'erreur est probablement causée par une spécification incorrecte du serveur de mise à jour (chemin réseau du dossier miroir) à partir duquel les postes de travail locaux téléchargent les mises à jour. Pour vérifier le dossier, cliquez sur (Windows) **Démarrer > Exécuter** entrez le nom du dossier et cliquez sur **OK**. Le contenu du dossier doit s'afficher.

ESET File Security **exige un nom d'utilisateur etun mot de passe** : l'erreur est probablement causée par l'entrée dans la section mise à jour de données d'authentification incorrectes (Nom d'utilisateur et Mot de passe). Le nom d'utilisateur et le mot de passe donnent accès au serveur de mise à jour, à partir duquel le programme se télécharge. Assurez-vous que les données d'authentification sont correctes et entrées dans le bon format. Par exemple, *Domaine/Nom d'utilisateur* ou *Workgroup/Nom d'utilisateur*, en plus des mots de passe correspondants. Si le serveur miroir est accessible à Tous, cela ne veut pas dire que tout utilisateur est autorisé à y accéder. « Tous » ne veut pas dire tout utilisateur non autorisé, cela veut tout simplement dire que le dossier est accessible à tous les utilisateurs du domaine. Par conséquent, si le dossier est accessible à Tous, un nom d'utilisateur du domaine et un mot de passe sont toujours nécessaires et doivent être entrés dans la configuration des mises à jour.

ESET File Security **signale une erreur de connexion au serveur miroir** - Le port de communication défini pour l'accès au miroir via HTTP est bloqué.

4.3.2 Comment créer des tâches de mise à jour

Vous pouvez déclencher les mises à jour manuellement en cliquant sur **Mettre à jour la base des signatures de virus** dans la fenêtre principale qui s'affiche lorsque vous cliquez sur Mettre à jour dans le menu principal.

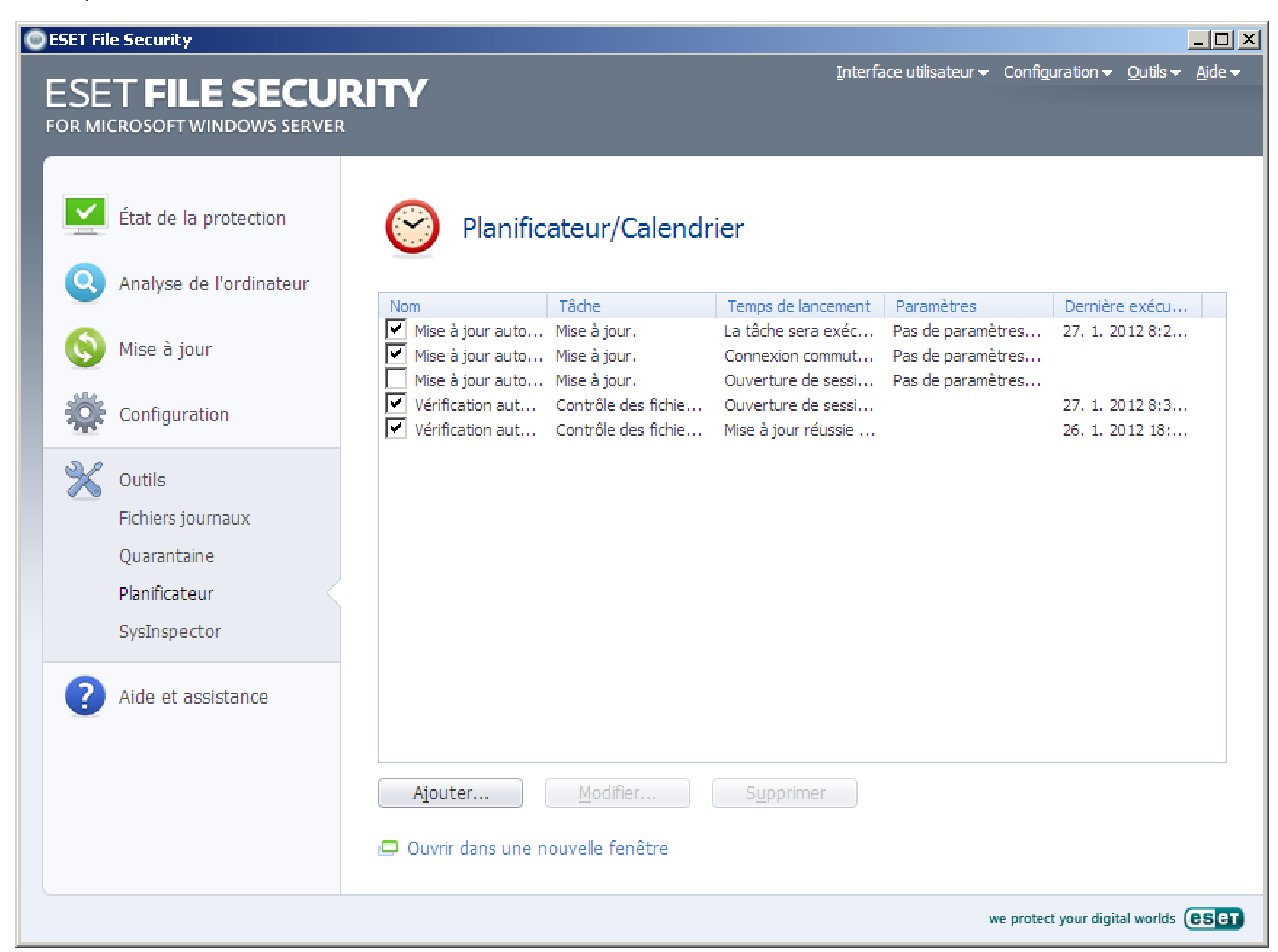
Les mises à jour peuvent également être exécutées sous forme de tâches planifiées. Pour configurer une tâche planifiée, cliquez sur **Outils** > **Planificateur**. Par défaut, les tâches suivantes sont activées dans ESET File Security :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**

Chaque tâche de mise à jour peut être modifiée selon les besoins de l'utilisateur. Outre les tâches de mise à jour par défaut, vous pouvez en créer des nouvelles avec vos propres paramètres. Pour plus d'informations sur la création et la configuration des tâches de mise à jour, reportez-vous à la section Planificateur.

4.4 Planificateur

Le planificateur est disponible si l'option Mode avancé dans ESET File Security est activée. Le **Planificateur** est accessible depuis le menu principal d'ESET File Security, dans **Outils**. Le planificateur contient la liste de toutes les tâches planifiées et des propriétés de configuration telles que la date et l'heure prédéfinies, ainsi que le profil d'analyse utilisé.



Par défaut, les tâches planifiées suivantes sont affichées dans le **Planificateur** :

- **Mise à jour automatique régulière**
- **Mise à jour automatique après une connexion commutée**
- **Mise à jour automatique après ouverture de session utilisateur**
- **Vérification automatique des fichiers de démarrage**
- **Vérification automatique des fichiers de démarrage après la mise à jour réussie de la base des signatures de virus**

Pour modifier la configuration d'une tâche planifiée existante (par défaut ou définie par l'utilisateur), cliquez avec le bouton droit sur la tâche et cliquez sur **Modifier...** Vous pouvez également sélectionner la tâche à modifier et cliquer sur le bouton **Modifier...**

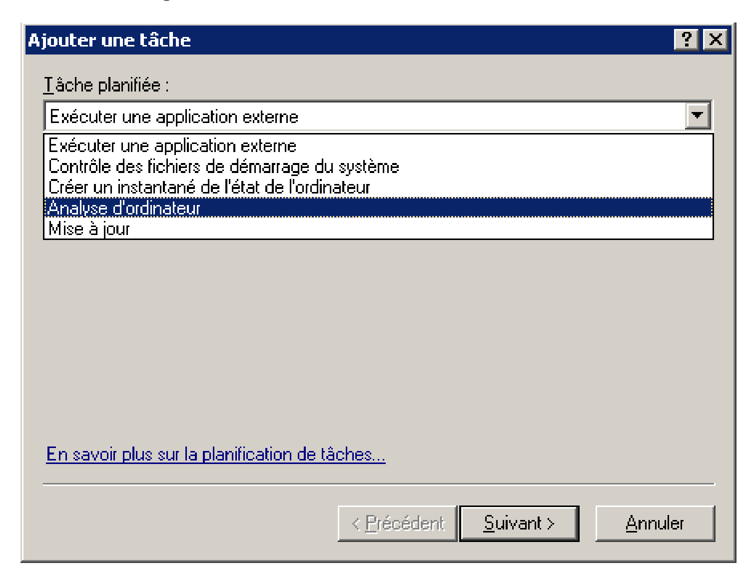
4.4.1 Pourquoi planifier des tâches ?

Le planificateur gère et lance les tâches planifiées qui ont été préalablement définies et configurées. La configuration et les propriétés comprennent des informations telles que la date et l'heure, ainsi que des profils spécifiques à utiliser pendant l'exécution de la tâche.

4.4.2 Création de nouvelles tâches

Pour créer une nouvelle tâche dans le planificateur, cliquez sur le bouton **Ajouter...** ou cliquez avec le bouton droit sur la tâche et sélectionnez **Ajouter...** dans le menu contextuel. Cinq types de tâches planifiées sont disponibles :

- **Exécuter une application externe**
- **Contrôle des fichiers de démarrage du système**
- **Créer un instantané du statut de l'ordinateur**
- **Analyse de l'ordinateur à la demande**
- **Mettre à jour**



La tâche planifiée la plus fréquente étant la **mise à jour**, nous allons expliquer comment ajouter une nouvelle tâche de mise à jour.

Dans le menu déroulant **Tâche planifiée** : , sélectionnez **Mettre à jour**. Cliquez sur **Suivant** et saisissez le nom de la tâche dans le champ **Nom de la tâche** : . Sélectionnez la fréquence de la tâche. Les options disponibles sont les suivantes : **Une fois**, **Plusieurs fois**, **Quotidiennement**, **Hebdo** et **Déclenchée par un événement**. Selon la fréquence sélectionnée, vous serez invité à choisir différents paramètres de mise à jour. Vous pouvez définir ensuite l'action à entreprendre si la tâche ne peut pas être effectuée ou terminée à l'heure planifiée. Les trois options suivantes sont disponibles :

- **Attendre le prochain moment planifié**
- **Exécuter la tâche dès que possible**
- **Exécuter la tâche immédiatement si le temps écoulé depuis la dernière exécution dépasse l'intervalle spécifié** (l'intervalle peut être défini à l'aide de la zone de liste déroulante Intervalle minimal entre deux tâches)

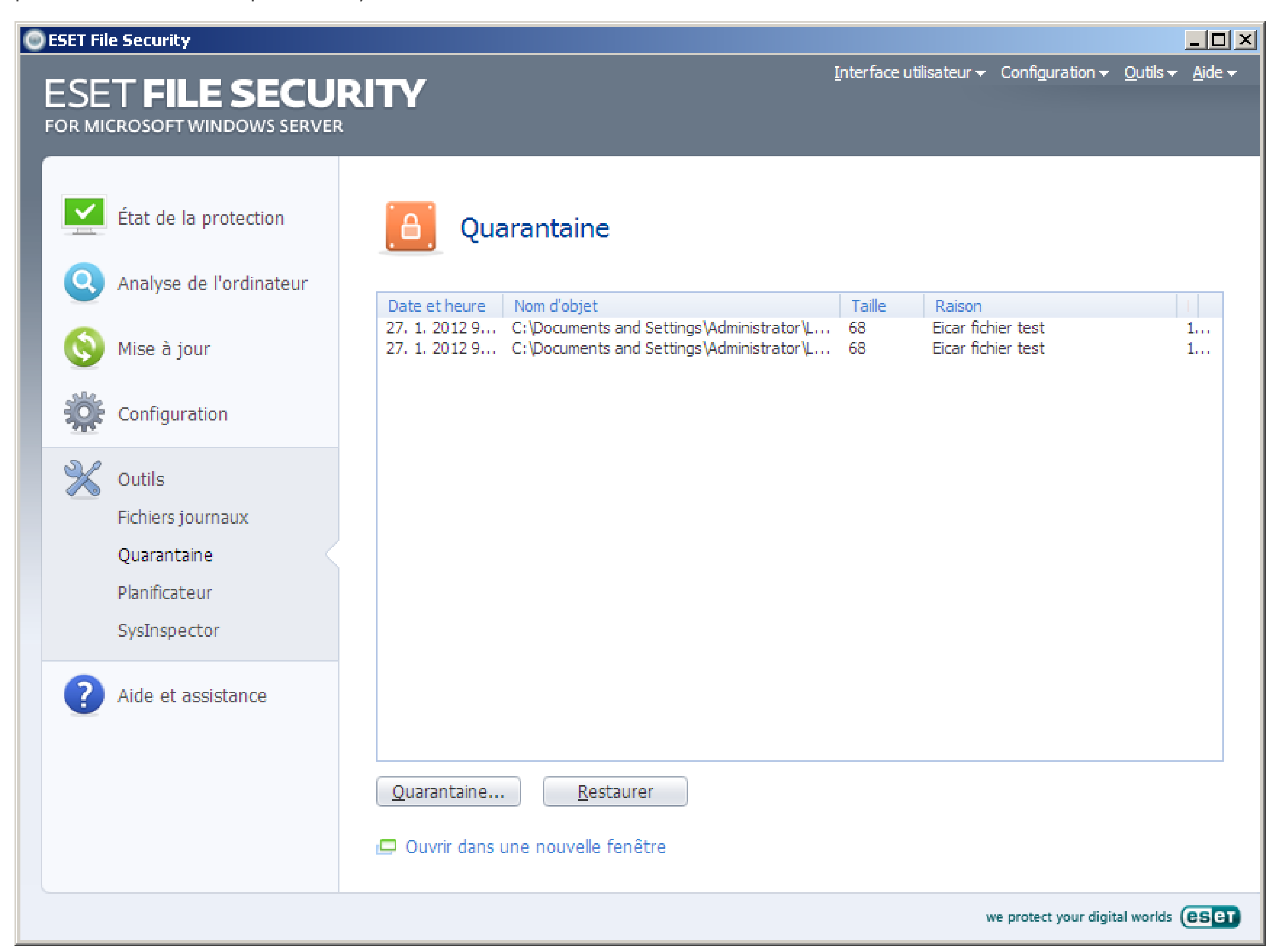
L'étape suivante affiche un résumé complet de la tâche planifiée courante ; l'option **Exécuter la tâche avec des paramètres spécifiques** doit être automatiquement activée. Cliquez sur le bouton **Terminer**.

La boîte de dialogue qui apparaît permet de sélectionner les profils à utiliser pour la tâche planifiée. L'utilisateur peut spécifier un profil principal et un profil secondaire qui sera utilisé si la tâche ne peut s'exécuter à l'aide du profil principal. Confirmez en cliquant sur **OK** dans la fenêtre **Profils de mise à jour**. La nouvelle tâche planifiée est ajoutée à la liste des tâches planifiées.

4.5 Quarantaine

La principale fonction de la quarantaine est le stockage en toute sécurité des fichiers infectés. Les fichiers doivent être placés en quarantaine s'ils ne peuvent pas être nettoyés, s'il est risqué ou déconseillé de les supprimer ou s'ils sont détectés erronément par ESET File Security.

Vous pouvez choisir de mettre n'importe quel fichier en quarantaine. Cette action est conseillée si un fichier se comporte de façon suspecte mais n'a pas été détecté par l'analyseur antivirus. Les fichiers de la quarantaine peuvent être soumis pour analyse au laboratoire de recherche sur les menaces d'ESET.



Les fichiers du dossier de quarantaine peuvent être visualisés dans un tableau qui affiche la date et l'heure de mise en quarantaine, le chemin de l'emplacement d'origine du fichier infecté, sa taille en octets, la raison (**ajouté par l'utilisateur...**), ainsi que le nombre de menaces (s'il s'agit par exemple d'une archive contenant plusieurs infiltrations).

4.5.1 Mise en quarantaine de fichiers

ESET File Security déplace automatiquement les fichiers supprimés en quarantaine (si vous n'avez pas annulé cette option dans la fenêtre d'alerte). Au besoin, vous pouvez mettre manuellement en quarantaine tout fichier suspect en cliquant sur le bouton **Quarantaine...** Dans ce cas, le fichier d'origine n'est pas supprimé de son emplacement initial. Il est également possible d'utiliser le menu contextuel à cette fin : cliquez avec le bouton droit dans la fenêtre **Quarantaine** et sélectionnez l'option **Ajouter...**

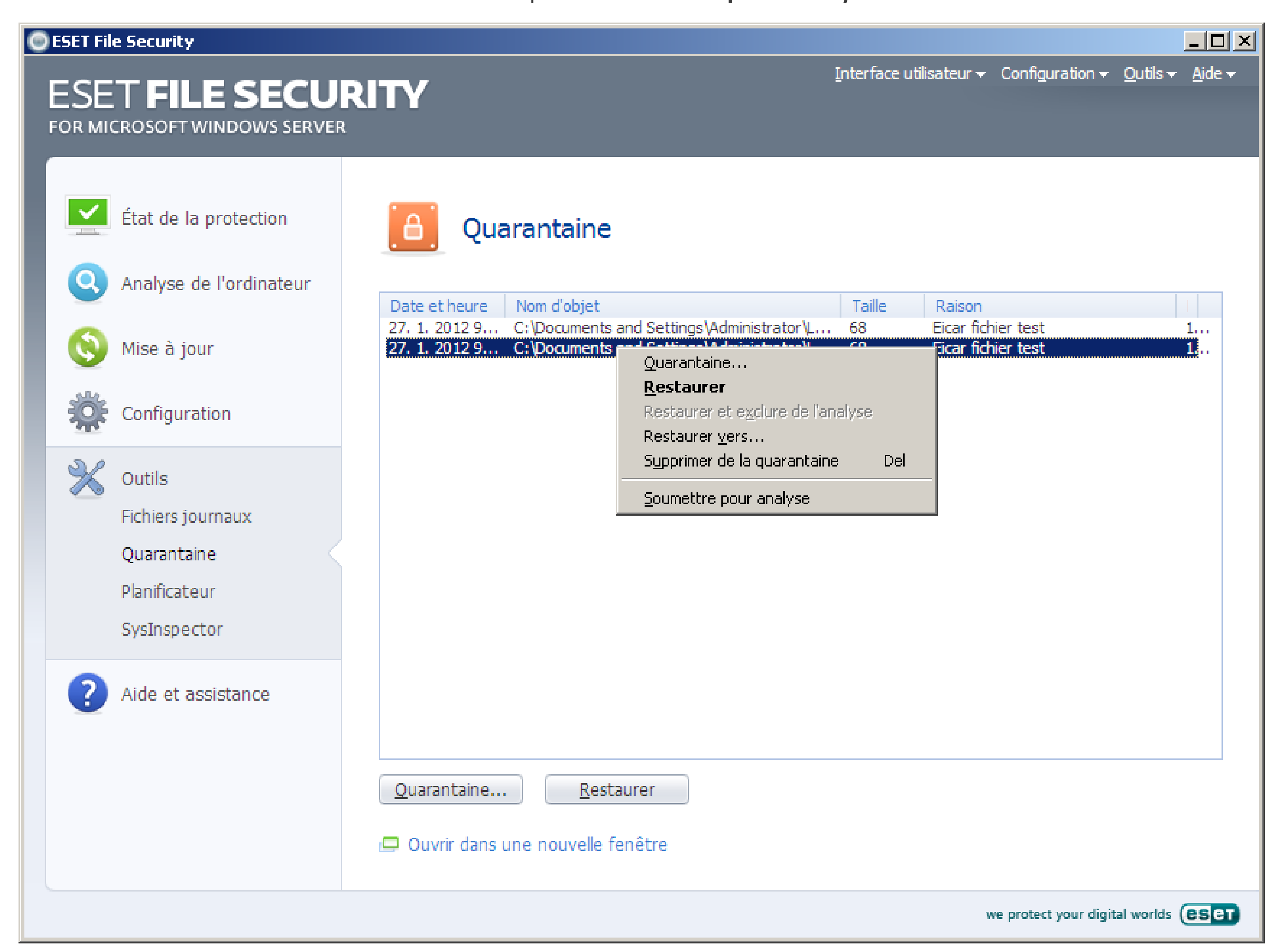
4.5.2 Restauration depuis la quarantaine

Les fichiers mis en quarantaine peuvent aussi être restaurés à leur emplacement d'origine. Utilisez la fonction **Restaurer** à cette fin. L'option **Restaurer** est disponible dans le menu contextuel accessible en cliquant avec le bouton droit sur le fichier dans le fenêtre Quarantaine. Le menu contextuel offre également l'option **Restaurer vers** qui permet de restaurer des fichiers vers un emplacement autre que celui d'origine dont ils ont été supprimés.

REMARQUE: si le programme place en quarantaine, par erreur, un fichier inoffensif, il convient de le restaurer, de l'exclure de l'analyse et de l'envoyer au service d'assistance d'ESET

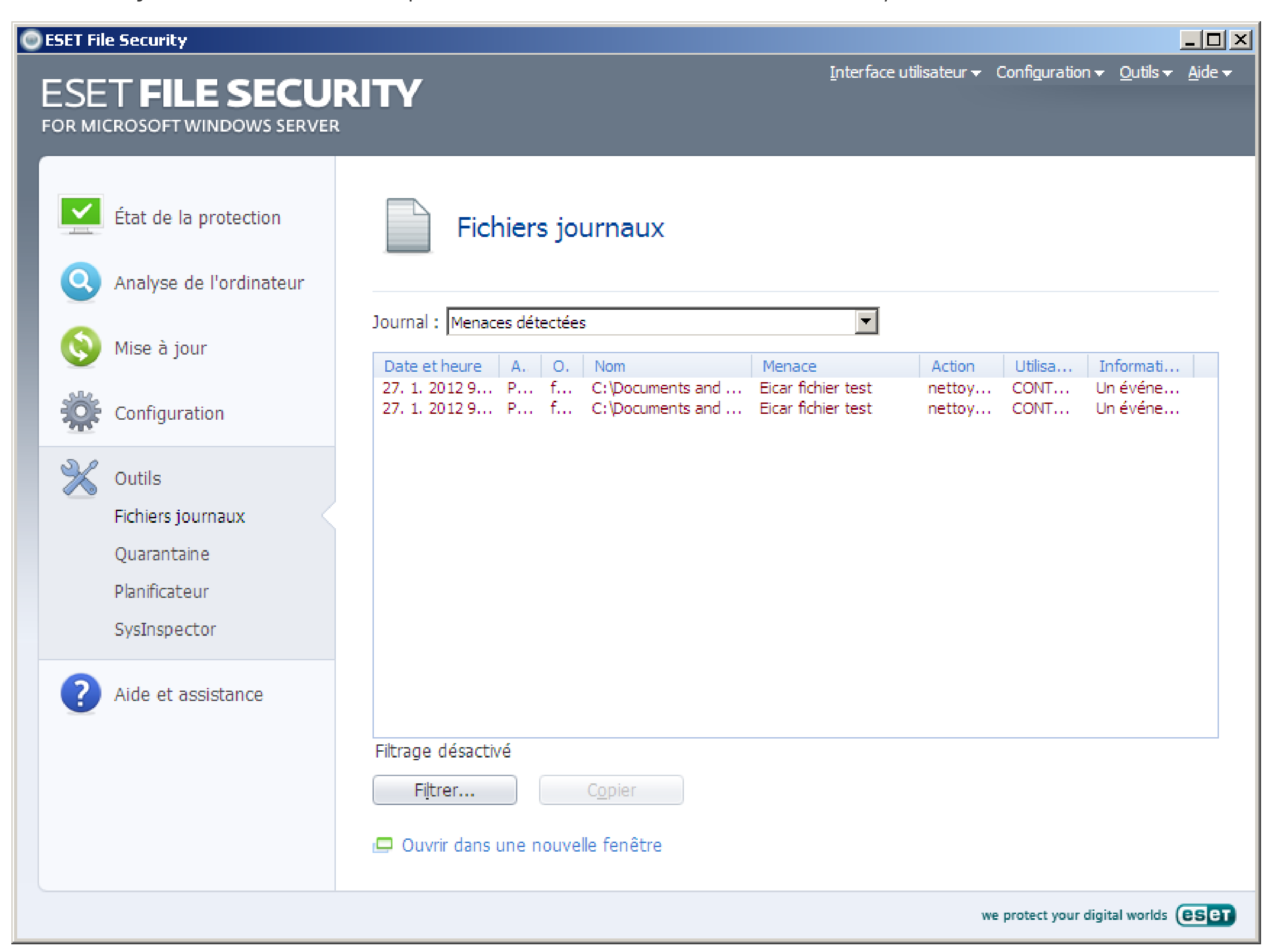
4.5.3 Soumission de fichiers de quarantaine

Si vous avez placé en quarantaine un fichier suspect non détecté par le programme ou si un fichier a été considéré par erreur comme étant infecté (par exemple par l'analyse heuristique du code) et placé en quarantaine, envoyez ce fichier au laboratoire de recherche sur les menaces d'ESET. Pour soumettre un fichier de la quarantaine, cliquez avec le bouton droit sur le fichier et sélectionnez l'option **Soumettre pour analyse** dans le menu contextuel.



4.6 Fichiers journaux

Les fichiers journaux contiennent tous les événements importants qui se sont produits et fournissent un aperçu des menaces détectées. La consignation représente un puissant outil pour l'analyse système, la détection de menaces et le dépannage. La consignation est toujours active en arrière-plan sans interaction de l'utilisateur. Les informations sont enregistrées en fonction des paramètres de détail actifs. Il est possible de consulter les messages texte et les journaux directement à partir de l'environnement ESET File Security.



Vous pouvez accéder aux fichiers journaux depuis le menu principal en cliquant sur **Outils** > **Fichiers journaux**. Sélectionnez le type d'enregistrement souhaité, puis cliquez sur le menu déroulant **Journal** dans la partie supérieure de la fenêtre. Les journaux suivants sont disponibles :

- **Menaces détectées** - cette option permet de consulter toutes les informations concernant les événements liés à la détection d'infiltrations, excepté les infiltrations détectées par l'analyse de l'ordinateur à la demande (ces événements sont enregistrés dans le journa **Analyse de l'ordinateur à la demande**).
- **Événements** : cette option permet aux administrateurs système et aux utilisateurs de résoudre des problèmes. Toutes les actions importantes exécutées par ESET File Security sont enregistrées dans les journaux des événements.
- **Analyse de l'ordinateur à la demande** : cette fenêtre affiche les résultats de toutes les analyses effectuées. Double-cliquez sur une entrée pour afficher les détails de l'analyse à la demande correspondante.

Vous pouvez copier les informations affichées dans chaque section directement dans le Presse-papiers en sélectionnant l'entrée souhaitée, puis en cliquant sur le bouton **Copier**. Pour sélectionner plusieurs entrées, utilisez les touches CTRL (sélection d'éléments non contigus) et MAJ (sélection d'éléments contigus).

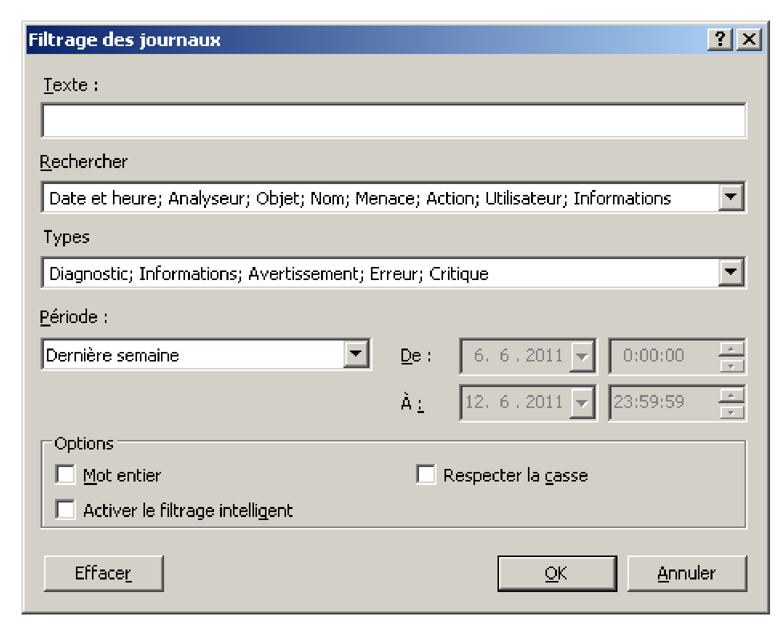
4.6.1 Filtrage des journaux

Le filtrage des journaux est une fonctionnalité très utile qui vous permet de rechercher des enregistrements dans les fichiers journaux, notamment lorsque les enregistrements sont très nombreux et qu'il est difficile de trouver les informations nécessaires.

Lorsque vous utilisez le filtrage, vous pouvez saisir une chaîne des éléments à filtrer dans **Rechercher**, spécifier les colonnes dans lesquelles effectuer la recherche dans **Rechercher dans les colonnes**, sélectionner les types d'enregistrement dans **Types d'enregistrements** et définir une heure dans la zone **Heure** afin de restreindre le nombre d'enregistrements. En indiquant certaines options de filtrage, vous pouvez afficher uniquement les enregistrements pertinents (en fonction de ces options) dans la fenêtre **Fichiers journaux** afin d'y accéder facilement.

Pour ouvrir la fenêtre **Filtrage des journaux**, appuyez une fois sur le bouton **Filtrer...** dans **Outils** > **Fichiers journaux** ou utilisez le raccourci clavier Ctrl + Maj + F.

REMARQUE : pour rechercher un enregistrement donné, utilisez plutôt la fonctionnalité Rechercher dans le journal , seule ou avec le filtrage des journaux.



En indiquant certaines options de filtrage, vous pouvez afficher uniquement les enregistrements pertinents (en fonction de ces options) dans la fenêtre Fichiers journaux. Le nombre d'enregistrements affichés est alors restreint, ce qui facilite la recherche des informations nécessaires. Plus vous utilisez d'options de filtrage, plus les résultats sont restreints.

Rechercher : saisissez une chaîne (mot ou partie de mot). Seuls les enregistrements contenant cette chaîne sont affichés. Les autres enregistrements sont masqués pour une meilleure lisibilité.

Rechercher dans les colonnes : : sélectionnez les colonnes à prendre en compte lors du filtrage. Vous pouvez cocher une ou plusieurs colonnes en tant que critères de filtrage. Par défaut, toutes les colonnes sont cochées :

- **Heure**
- **Module**
- **Événement**
- **utilisateur**

Types d'enregistrements : : vous permet de choisir le type d'enregistrements à afficher. Vous pouvez choisir un type d'enregistrement en particulier, plusieurs types simultanément ou tous les types (option par défaut) :

- **Diagnostic**
- **Informations**
- **Avertissement**
- **Erreur**
- **Critique**

Période : : utilisez cette option pour filtrer les enregistrements par période. Vous pouvez choisir l'une des options suivantes :

- **Journal complet** (option par défaut) : aucun filtrage par période n'est effectué et l'intégralité du journal est affiché.
- **Jour antérieur**
- **Dernière semaine**
- **Dernier mois**
- **Intervalle** : en sélectionnant un intervalle, vous pouvez indiquer la période exacte (date et heure) afin de n'afficher que les enregistrements correspondant à la période indiquée.

Outre les paramètres de filtrage ci-dessus, vous disposez également plusieurs **Options** :

Mot entier : affiche uniquement les enregistrements qui correspondent à la chaîne sous forme de mot entier indiquée dans la zone de **recherche**.

Respecter la casse : affiche uniquement les enregistrements qui correspondent à l'utilisation des majuscules et des minuscules indiquée dans la zone de **recherche**.

Activer le filtrage intelligent : utilisez cette option pour qu'ESET File Security puisse effectuer le filtrage à l'aide de ses propres méthodes.

Lorsque la configuration des options de filtrage est terminée, appuyez sur le bouton **OK** pour appliquer le filtrage. La fenêtre **Fichiers journaux** n'affiche que les enregistrements correspondants en fonction des options de filtre.

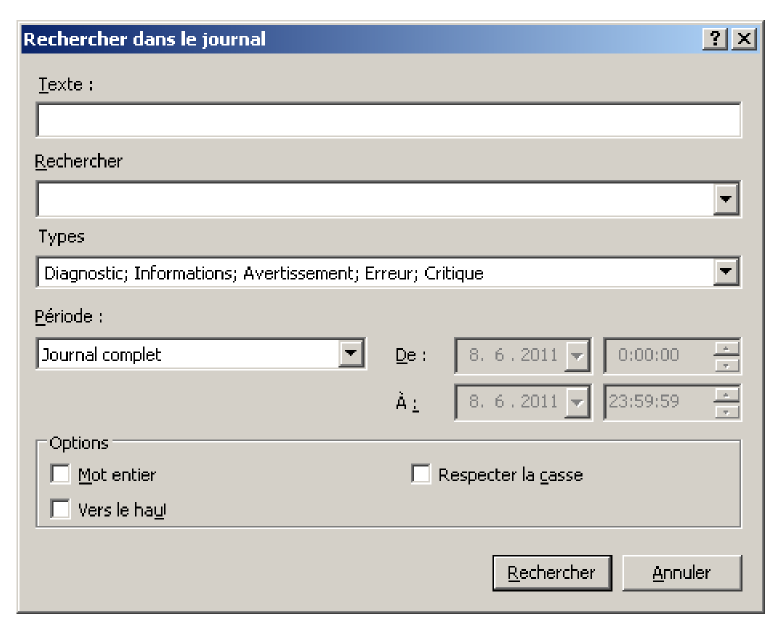
4.6.2 Rechercher dans le journal

Outre le filtrage des journaux, vous pouvez utiliser la fonctionnalité de recherche dans les fichiers journaux. Toutefois, vous pouvez également l'utiliser indépendamment du filtrage des journaux. Ce procédé est utile lorsque vous recherchez des enregistrements précis dans les journaux. Tout comme le filtrage des journaux, cette fonctionnalité de recherche permet de trouver les informations que vous recherchez, notamment lorsque les enregistrements sont très nombreux.

Lorsque vous utilisez la fonction de recherche dans le journal, vous pouvez saisir une chaîne des éléments à filtrer dans **Rechercher**, spécifier les colonnes dans lesquelles effectuer la recherche dans **Rechercher dans les colonnes**, sélectionner les types d'enregistrement dans **Types d'enregistrement** et définir une heure dans **Heure** afin de ne rechercher que les enregistrements correspondant à la période indiquée. En indiquant certaines options de recherche, vous pouvez afficher uniquement les enregistrements pertinents (en fonction de ces options) dans la fenêtre Fichiers journaux.

Pour effectuer des recherches dans les journaux, ouvrez la fenêtre **Rechercher dans le journal** en appuyant sur les touches Ctrl + F.

REMARQUE : vous pouvez utiliser la fonctionnalité Rechercher dans le journal avec le filtrage des journaux. Vous pouvez d'abord restreindre le nombre d'enregistrements à l'aide du filtrage des journaux, puis effectuer une recherche uniquement dans les enregistrements filtrés.



Rechercher : saisissez une chaîne (mot ou partie de mot). Seuls les enregistrements contenant cette chaîne sont trouvés. Les autres enregistrements sont ignorés.

Rechercher dans les colonnes : : sélectionnez les colonnes à prendre en compte lors de la recherche. Vous pouvez cocher une ou plusieurs colonnes à utiliser pour la recherche. Par défaut, toutes les colonnes sont cochées :

- **Heure**
- **Module**
- **Événement**
- **utilisateur**

Types d'enregistrements : : vous permet de choisir le type d'enregistrements à rechercher. Vous pouvez choisir un type d'enregistrement en particulier, plusieurs types simultanément ou tous les types (option par défaut) :

- **Diagnostic**
- **Informations**
- **Avertissement**
- **Erreur**
- **Critique**

Période : : utilisez cette option pour rechercher des enregistrements correspondant à une période. Vous pouvez choisir l'une des options suivantes :

- **Journal complet** (option par défaut) : n'effectue aucune recherche dans la période ; effectue une recherche dans l'intégralité du journal.
- **Jour antérieur**
- **Dernière semaine**
- **Dernier mois**
- **Intervalle** : en sélectionnant un intervalle, vous pouvez indiquer la période exacte (date et heure) afin de ne rechercher que les enregistrements correspondant à la période indiquée.

Outre les paramètres de recherche ci-dessus, vous disposez également plusieurs **Options** :

Mot entier : recherche uniquement les enregistrements qui correspondent à la chaîne sous forme de mot entier indiquée dans la zone de **recherche**.

Respecter la casse : recherche uniquement les enregistrements qui correspondent à l'utilisation des majuscules et des minuscules indiquée dans la zone de **recherche**.

Vers le haut : lance la recherche vers le haut.

Après avoir configuré les options de recherche, cliquez sur le bouton **Rechercher** pour lancer la recherche. La recherche s'arrête au premier enregistrement correspondant. Cliquez de nouveau sur le bouton **Rechercher** pour poursuivre la recherche. La recherche dans les fichiers journaux s'effectue de haut en bas, à partir de la position actuelle (de l'enregistrement sélectionné).

4.6.3 Maintenance des journaux

La configuration de la consignation d'ESET File Security est accessible à partir de la fenêtre principale du programme. Cliquez sur **Configuration** > **Accéder à la configuration avancée complète...** > **Outils** > **Fichiers journaux**. Les options suivantes peuvent être spécifiées pour les fichiers journaux :

- **Supprimer automatiquement les entrées** : les entrées journaux plus anciennes que le nombre de jours spécifié sont automatiquement supprimées.

- **Optimiser automatiquement les fichiers journaux** : permet la défragmentation automatique des fichiers journaux si le pourcentage spécifié d'enregistrements inutilisés est dépassé.

- **Verbosité minimale des journaux** : indique la verbosité minimale des journaux. Les options disponibles sont les suivantes :

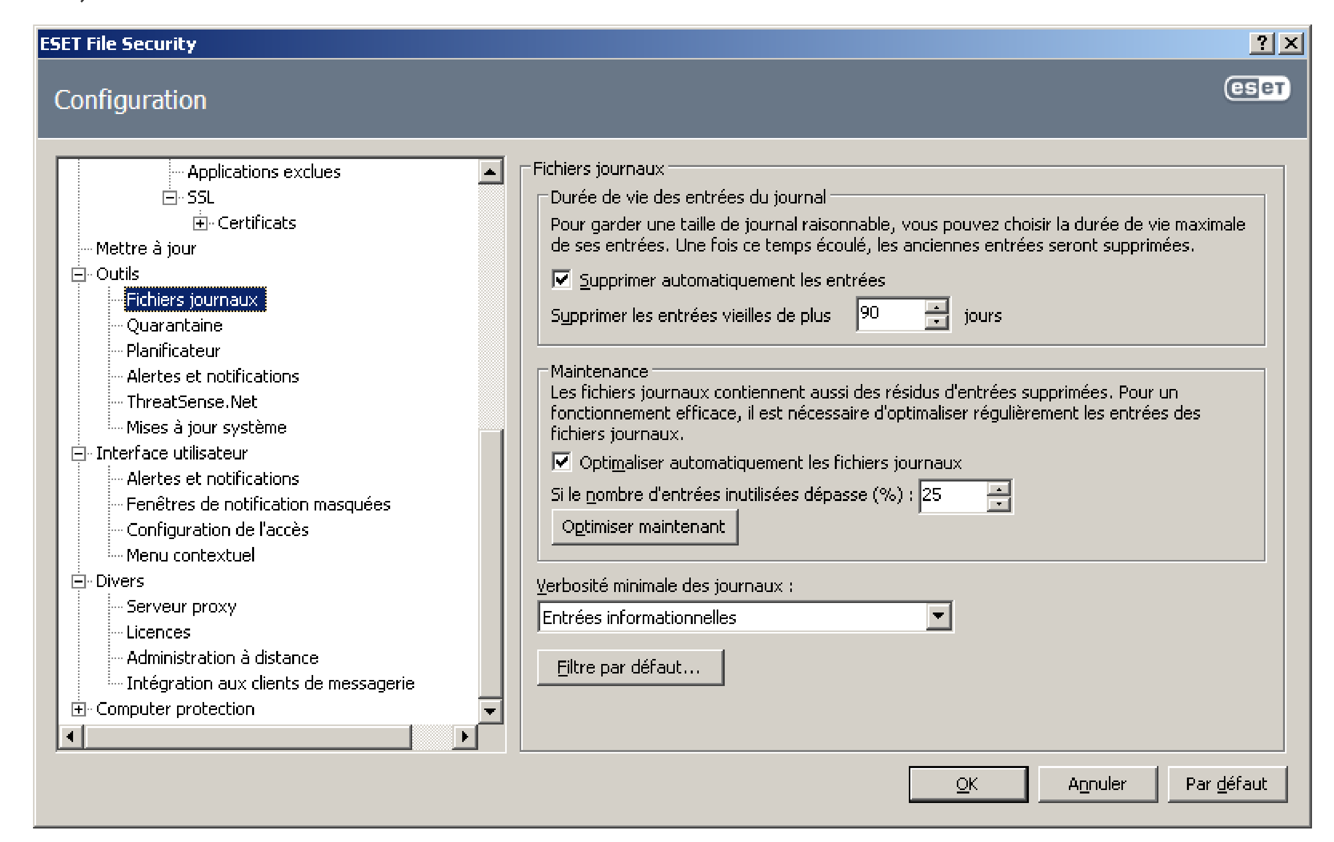
- **Entrées diagnostiques** : consigne toutes les informations nécessaires pour un réglage détaillé du programme et de toutes les entrées ci-dessus.

- **Entrées informatives** : enregistre tous les messages d'information, y compris les messages de mises à jour réussies et toutes les entrées ci-dessus.

- **Avertissements** : enregistre les erreurs critiques, les erreurs et les messages d'avertissement.

- **Erreurs** : les erreurs de type « Erreur de téléchargement de fichier » et les erreurs critiques sont enregistrées.

- **Avertissements critiques** : répertorie toutes les erreurs critiques (erreur de démarrage de la protection antivirus, etc.).



4.7 ESET SysInspector

4.7.1 Introduction à ESET SysInspector

ESET SysInspector est une application qui inspecte votre ordinateur en profondeur et qui affiche en détail toutes les données obtenues. Des informations telles que les pilotes et applications installés, les connexions réseau ou les entrées de registre importantes peuvent vous aider à élucider un comportement suspect du système, qu'il soit dû à une incompatibilité logicielle ou matérielle, ou à une infection par logiciel malveillant.

Vous pouvez accéder à ESET SysInspector de deux manières : Depuis la version intégrée dans les solutions ESET Security ou en téléchargeant gratuitement la version autonome (SysInspector.exe) depuis le site Internet d'ESET. Les deux versions sont identiques en matière de fonctionnalités et disposent des mêmes contrôles de programme. La seule différence réside dans la façon dont les résultats sont gérés. Les versions autonomes et intégrées vous permettent d'exporter des instantanés du système dans un fichier *.xml* et de les enregistrer sur le disque. Toutefois, la version intégrée vous permet également de stocker vos instantanés système directement dans **Outils** > **ESET SysInspector** (excepté ESET Remote Administrator). Pour plus d'informations, reportez-vous à la section ESET SysInspector en tant que partie de ESET File Security.

Veuillez patienter pendant que ESET SysInspector analyse votre ordinateur. L'analyse peut prendre entre 10 secondes et quelques minutes, en fonction de la configuration de votre matériel, du système d'exploitation et du nombre d'applications installées sur votre ordinateur.

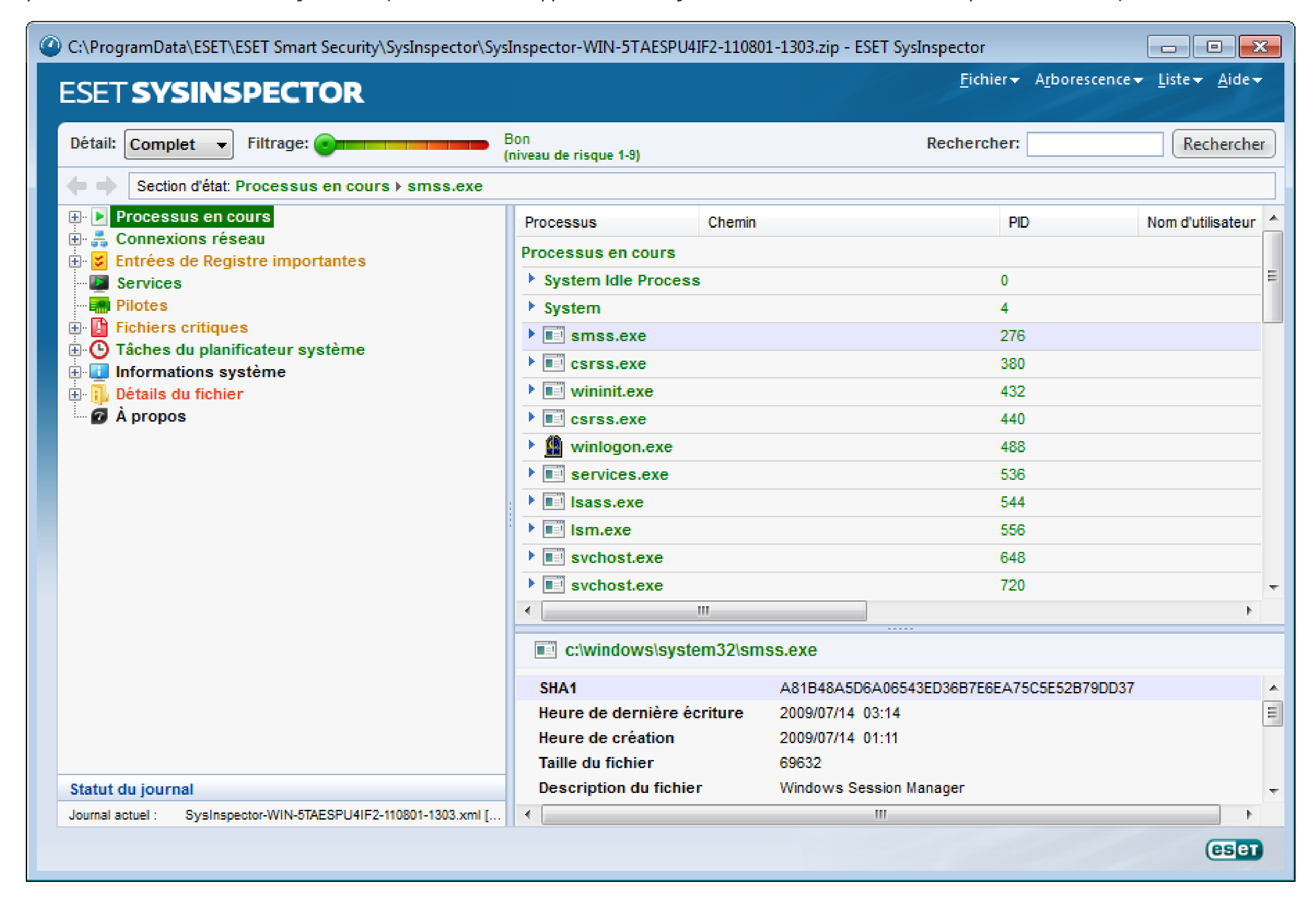
4.7.1.1 Démarrage d'ESET SysInspector

Pour démarrer ESET SysInspector, il suffit de lancer le fichier exécutable *SysInspector.exe* téléchargé depuis le site Web d'ESET. Si vous avez déjà installé une des solutions de sécurité ESET Security, vous pouvez exécuter ESET SysInspector directement depuis le menu Démarrer (**Programmes** > **ESET** > **ESET File Security**).

Patientez pendant que l'application vérifie le système, une opération qui pourrait durer plusieurs minutes en fonction du matériel et des données à recueillir.

4.7.2 Interface utilisateur et utilisation de l'application

Pour des raisons de clarté, la fenêtre principale est divisée en quatre principales sections : les Contrôles du programme situés dans le haut de la fenêtre principale, la fenêtre Navigation à gauche, la fenêtre Description à droite au centre et la fenêtre Détails à droite au bas de la fenêtre principale. La section État du journal énumère les paramètres de base d'un journal (filtre utilisé, type de filtre, journal résultat d'une comparaison, etc.).



4.7.2.1 Contrôles du programme

Cette section contient la description de tous les contrôles du programme disponible dans ESET SysInspector.

Fichier

En cliquant sur **Fichier**, vous pouvez enregistrer l'état actuel du système en vue d'une enquête ultérieure ou ouvrir un journal déjà enregistré. Pour la publication, il est conseillé de créer un journal **approprié pour envoi**. Sous cette forme, le journal omet les informations sensibles (nom d'utilisateur, nom d'ordinateur, nom de domaine, privilèges actuels de l'utilisateur, variables d'environnement, etc.).

REMARQUE : vous pouvez ouvrir des rapports enregistrés de ESET SysInspector en les faisant glisser et en les déposant sur la fenêtre principale.

Arborescence

Permet de développer ou de réduire tous les nœuds et d'exporter les sections sélectionnées dans le script de service.

Liste

Contient des fonctions qui simplifient la navigation dans le programme, ainsi que d'autres fonctionnalités comme l'obtention d'informations en ligne.

Aide

Contient des informations sur l'application et ses fonctions.

Détails

Ce paramètre détermine les informations affichées dans la fenêtre principale afin de simplifier l'utilisation des informations. En mode de base, vous avez accès aux informations utilisées pour trouver les solutions aux problèmes communs dans votre système. En mode Moyen, le programme affiche moins de détails. En mode Complet, ESET SysInspector indique toutes les informations requises pour résoudre des problèmes très particuliers.

Filtrage des éléments

Le filtrage des éléments est particulièrement adapté à la recherche de fichiers suspects ou d'entrées de Registre dans le système. En déplaçant le curseur, vous pouvez filtrer les éléments en fonction de leur niveau de risque. Si le curseur est positionné tout à fait à gauche (Niveau de risque 1), tous les éléments sont affichés. En déplaçant le curseur vers la droite, l'application filtre tous les éléments dont le risque est inférieur au niveau de risque actuel et affiche uniquement les éléments qui sont plus suspects que le niveau affiché. Si le curseur est en position maximale à droite, le programme affiche uniquement les éléments nuisibles connus.

Tous les éléments qui appartiennent aux catégories de risque 6 à 9 peuvent poser un risque pour la sécurité. Si vous n'utilisez pas certaines des solutions de sécurité d'ESET, nous vous conseillons d'analyser votre système à l'aide d' ESET Online Scanner dans le cas où ESET SysInspector détecte un élément de ce genre. ESET Online Scanner est un service gratuit.

REMARQUE : le niveau de risque d'un élément peut être rapidement déterminé grâce à la couleur que prend le curseur pour indiquer le niveau de risque.

Rechercher

La fonction de recherche permet de trouver rapidement un élément sur la base de son nom ou d'une partie de son nom. Les résultats de la recherche sont affichés dans la fenêtre Description.

Retour

En cliquant sur la flèche arrière ou avant, vous pouvez revenir aux informations affichées précédemment dans la fenêtre Description. Vous pouvez utiliser la touche de retour arrière et la barre d'espace au lieu de cliquer sur les flèches arrière ou avant.

Section d'état

Affiche le nœud actuel dans la fenêtre Navigation.

Important : les éléments surlignés en rouge sont inconnus et c'est la raison pour laquelle l'application les marque comme potentiellement dangereux. Si un élément est rouge, cela ne signifie pas automatiquement que vous pouvez supprimer le fichier. Avant de le supprimer, assurez-vous que les fichiers sont bel et bien dangereux ou qu'ils ne sont pas nécessaires.

4.7.2.2 Navigation dans ESET SysInspector

ESET SysInspector répartit divers types d'informations en plusieurs sections principales baptisées nœuds. Si des détails supplémentaires sont disponibles, vous pouvez les afficher en développant chaque nœud en sous-nœuds. Pour développer ou réduire un nœud, double-cliquez sur son nom, ou cliquez sur ⊞ ou sur ⊟ en regard du nom du nœud. Quand vous parcourez la structure arborescente des nœuds et des sous-nœuds dans la fenêtre de navigation, vous pouvez voir différents détails pour chaque nœud dans la fenêtre Description. Si vous parcourez les éléments de la fenêtre Description, des détails supplémentaires pour chaque élément peuvent être affichés dans la fenêtre Détails.

Voici les descriptions des principaux nœuds de la fenêtre Navigation et des informations qui s'y rapportent dans les fenêtres Description et Détails.

Processus en cours

Ce nœud comprend les informations sur les applications et les processus en cours d'exécution au moment de la création du journal. La fenêtre Détails comprend des détails complémentaires pour chaque processus tels que les bibliothèques dynamiques utilisées par les processus et leur emplacement dans le système, le nom de l'éditeur de l'application et le niveau de risque du fichier.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

REMARQUE : Un système d'exploitation comprend plusieurs composants noyaux importants fonctionnant 24 h. sur 24/7 j. sur 7 et assurant des fonctions de base et vitales pour d'autres applications utilisateur. Dans certains cas, ces processus sont repris dans l'outil ESET SysInspector avec un chemin d'accès au fichier commençant par \??\. Ces symboles garantissent l'optimisation préalable au lancement pour ce processus ; ils ne présentent aucun danger pour le système.

Connexions de réseau

La fenêtre Description contient la liste des processus et des applications qui communiquent via le réseau à l'aide du protocole sélectionné dans la fenêtre navigation (TCP ou UDP), ainsi que l'adresse distante à laquelle l'application est connectée. Vous pouvez également vérifier les adresses IP des serveurs DNS.

La fenêtre Détails contient des informations complémentaires sur les éléments sélectionnés dans la fenêtre Description telles que la taille du fichier ou son hachage.

Entrées de Registre importantes

Contient la liste des entrées de Registre sélectionnées qui sont souvent liées à des problèmes système. Il s'agit des entrées qui indiquent les applications de démarrage, les objets d'application d'assistance du navigateur, etc.

La fenêtre Description peut indiquer les fichiers en rapport avec les entrées de Registre particulières. La fenêtre Détails peut également présenter des détails supplémentaires.

Services

La fenêtre Description contient la liste des fichiers enregistrés en tant que services Windows. Vous pouvez contrôler la manière dont le démarrage du service est paramétré, ainsi que des détails spécifiques du fichier dans la fenêtre Détails.

Pilotes

Liste des pilotes installés sur le système.

Fichiers critiques

La fenêtre Description affiche le contenu des fichiers critiques liés au système d'exploitation Microsoft Windows.

Tâches du planificateur système

Contient une liste de tâches déclenchées par le Planificateur de tâches de Windows à une heure précise ou selon un intervalle spécifié.

Informations système

Contient des informations détaillées sur le matériel et le logiciel, ainsi que des informations sur les variables d'environnement définies, les droits de l'utilisateur et les journaux d'événements du système.

Détails du fichier

Liste des fichiers système importants et des fichiers du dossier Program Files. Des informations complémentaires spécifiques sur les fichiers sont disponibles dans les fenêtres Description et Détails.

À propos de

Informations sur la version de ESET SysInspector et la liste des modules du programme.

4.7.2.2.1 Raccourcis clavier

Voici les raccourcis clavier disponibles dans ESET SysInspector :

Fichier

Ctrl+O	ouvre un journal existant
Ctrl+S	enregistre les journaux créés

Générer

Ctrl+G	génère un instantané standard du statut de l'ordinateur
Ctrl+H	génère un instantané du statut de l'ordinateur qui peut également journaliser des informations sensibles

Filtrage des éléments

1, O	affiche les éléments de niveau de risque 1 à 9 (acceptable)
2	affiche les éléments de niveau de risque 2 à 9 (acceptable)
3	affiche les éléments de niveau de risque 3 à 9 (acceptable)
4, U	affiche les éléments de niveau de risque 4 à 9 (inconnu)
5	affiche les éléments de niveau de risque 5 à 9 (inconnu)
6	affiche les éléments de niveau de risque 6 à 9 (inconnu)
7, B	affiche les éléments de niveau de risque 7 à 9 (risqué)
8	affiche les éléments de niveau de risque 8 à 9 (risqué)
9	affiche les éléments de niveau de risque 9 (risqué)
-	diminue le niveau de risque
+	augmente le niveau de risque
Ctrl+9	mode de filtrage, niveau égal ou supérieur
Ctrl+0	mode de filtrage, niveau égal uniquement

Afficher

Ctrl+5	afficher par éditeur, tous les éditeurs
Ctrl+6	afficher par éditeur, uniquement Microsoft
Ctrl+7	afficher par éditeur, tous les autres éditeurs
Ctrl+3	afficher tous les détails
Ctrl+2	afficher les détails de précision moyenne
Ctrl+1	affichage de base
Retour arrière	revient une étape en arrière
Barre d'espace	avance d'une étape
Ctrl+W	développe l'arborescence
Ctrl+Q	réduit l'arborescence

Autres commandes

Ctrl+T	accède à l'emplacement d'origine de l'élément après la sélection dans les résultats de recherche
Ctrl+P	affiche des informations élémentaires sur un élément
Ctrl+A	affiche des informations complètes sur un élément
Ctrl+C	copie l'arborescence de l'élément
Ctrl+X	copie les éléments
Ctrl+B	trouve des informations sur les fichiers sélectionnés sur Internet
Ctrl+L	ouvre le dossier où se trouve le fichier sélectionné.
Ctrl+R	ouvre l'entrée correspondante dans l'éditeur de registre
Ctrl+Z	copie un chemin d'accès à un fichier (si l'élément est lié à un fichier)
Ctrl+F	passe au champ de recherche
Ctrl+D	ferme les résultats de la recherche
Ctrl+E	exécute le script de service

Comparaison

Ctrl+Alt+O	ouvre le journal d'origine/de comparaison

Ctrl+Alt+R	annule la comparaison
Ctrl+Alt+1	affiche tous les éléments
Ctrl+Alt+2	affiche uniquement les éléments ajoutés ; le journal indique les éléments présents dans le journal actuel
Ctrl+Alt+3	affiche uniquement les éléments supprimés ; le journal indique les éléments présents dans le journal précédent
Ctrl+Alt+4	affiche uniquement les éléments remplacés (fichiers inclus)
Ctrl+Alt+5	affiche uniquement les différences entre les journaux
Ctrl+Alt+C	affiche la comparaison
Ctrl+Alt+N	affiche le journal actuel
Ctrl+Alt+P	ouvre le journal précédent

Divers

F1	afficher l'aide
Alt+F4	quitter l'application
Alt+Maj+F4	quitter l'application sans demander
Ctrl+I	statistiques du journal

4.7.2.3 Comparer

La fonctionnalité Comparer permet de comparer deux journaux. Cette fonctionnalité met en évidence les éléments qui ne sont pas communs aux deux journaux. Cet outil est utile si vous souhaitez assurer le suivi des modifications dans le système. Il vous permettra de détecter l'activité d'un code malveillant.

Après son lancement, l'application crée un journal qui apparaît dans une nouvelle fenêtre. Accédez au menu **Fichier** > **Enregistrer le journal** pour enregistrer le journal dans un fichier. Vous pouvez ouvrir et afficher les fichiers journaux ultérieurement. Pour ouvrir un journal existant, sélectionnez **Fichier** > **Ouvrir le journal**. Dans la fenêtre principale de l'application, ESET SysInspector affiche toujours un journal à la fois.

En comparant deux journaux, vous pouvez afficher un journal actif et un autre journal enregistré dans un fichier. Pour comparer des journaux, choisissez l'option **Fichier** > **Comparer les journaux**, puis choisissez **Sélectionner un fichier**. Le journal sélectionné est comparé au journal actif dans les fenêtres principales de l'application. Le journal comparatif n'indiquera que les différences entre ces deux journaux.

REMARQUE : si vous comparez deux fichiers journaux, choisissez **Fichier** > **Enregistrer le journal** pour l'enregistrer dans un fichier ZIP. Les deux fichiers sont enregistrés. Si vous ouvrez ce fichier ultérieurement, les journaux qu'il contient seront comparés automatiquement.

En regard des éléments affichés, ESET SysInspector ajoute des symboles qui identifient les différences entre les journaux comparés.

Les éléments marqués par - se trouvent uniquement dans le journal actif et sont absents du journal de comparaison ouvert. Les éléments marqués du signe + ne figurent que dans le journal ouvert et sont absents du journal actif.

Description de tous les symboles qui peuvent être affichés à côté des éléments :

- + nouvelle valeur, absente du journal précédent.
- cette section de l'arborescence contient de nouvelles valeurs.
- - valeur supprimée, présente uniquement dans le journal précédent.
- cette section de l'arborescence contient des valeurs supprimées.
- valeur/fichier modifié.
- cette section de l'arborescence contient des valeurs/fichiers modifiés.
- le niveau de risque a diminué/était supérieur dans le journal précédent.
- le niveau de risque a augmenté/il était inférieur dans le journal précédent.

La section d'explication affichée dans le coin inférieur gauche décrit tous les symboles et affiche le nom des journaux comparés.

Statut du journal

Journal actuel : SysInspector-WIN-5TAESPU4IF2-110801-1316.xml [Chargé-ZIP]
Journal précédent : SysInspector-WIN-5TAESPU4IF2-110801-1303.xml [Chargé-ZIP]
Comparer : [Résultat de la comparaison]

Comparer la légende des icônes

+ Élément ajouté
− Élément supprimé
Fichier remplacé
L'état a été abaissé
L'état a été élevé
Élément(s) ajouté(s) dans la branche
Élément(s) supprimé(s) de la branche
Élément(s) ajouté(s) ou supprimé(s) dans la branche
Fichier(s) remplacé(s) dans la branche

Les journaux de comparaison peuvent être enregistrés dans un fichier et ouverts ultérieurement :

Exemple

Créez un journal reprenant les informations d'origine du système et enregistrez-le dans un fichier appelé précédent. xml. Après avoir modifié le système, ouvrez ESET SysInspector pour qu'il crée un nouveau journal. Enregistrez ce journal sous le nom *actuel.xml*.

Pour voir les différences entre ces deux journaux, utilisez l'option **Fichier** > **Comparer les journaux**. Le programme crée un journal de comparaison qui indique les différences entre les journaux.

Un résultat identique peut être obtenu si vous utilisez l'option de ligne de commande suivante :

SysInspector.exe actuel.xml précédent.xml

4.7.3 Paramètres de la ligne de commande

ESET SysInspector prend en charge la création de rapports via la ligne de commande à l'aide de ces paramètres :

/gen	crée un journal directement depuis la ligne de commande sans exécuter l'interface utilisateur.
/privacy	crée un journal qui exclut les informations sensibles.
/zip	stocke le journal obtenu directement sur le disque dans un fichier compressé.
/silent	supprime l'affichage de la barre de progression de la création du journal.
/help, /?	affiche des informations sur les paramètres de la ligne de commande.

Exemples

Pour charger un journal en particulier directement dans le navigateur, saisissez : *SysInspector.exe "c:\clientlog.xml"*
Pour créer un journal à l'emplacement actuel, saisissez : *SysInspector.exe /gen*
Pour créer un journal dans un dossier en particulier, saisissez : *SysInspector.exe /gen="c:\dossier\"*
Pour créer un journal dans un fichier/dossier en particulier, saisissez : *SysInspector.exe /gen="c:\dossier\monnouveaujournal.xml"*
Pour créer un journal qui exclut les informations sensibles directement dans un fichier compressé, saisissez : *SysInspector.exe /gen="c:\monnouveaujournal.zip"/privacy/zip*
Pour comparer deux journaux, utilisez : *SysInspector.exe "actuel.xml" "original.xml"*

REMARQUE : si le nom du fichier/dossier contient un espace, saisissez-le entre guillemets.

4.7.4 Script de service

Le script de service est un outil qui vise à offrir une aide aux clients qui utilisent ESET SysInspector en supprimant les objets indésirables du système.

Le script de service permet à l'utilisateur d'exporter l'ensemble du journal ESET SysInspector ou des parties sélectionnées uniquement. Après l'exportation, vous pouvez marquer des objets indésirables pour suppression. Vous pouvez ensuite exécuter le journal modifié pour supprimer les objets marqués.

Le script de service convient aux utilisateurs expérimentés qui connaissent les problèmes des systèmes de diagnostic. Des modifications non qualifiées peuvent endommager le système d'exploitation.

Exemple

si vous pensez que votre ordinateur est infecté par un virus qui n'est pas détecté par votre logiciel antivirus, suivez les instructions ci-après :

- Exécutez ESET SysInspector pour obtenir un nouvel instantané du système.
- Sélectionnez le premier élément de la section à gauche (dans l'arborescence), appuyez sur la touche Ctrl, puis sélectionnez le dernier élément afin de marquer tous les éléments.
- Cliquez avec le bouton droit sur les objets sélectionnés, puis sélectionnez l'option du menu contextuel **Exporter les sections sélectionnées dans un script de service**.
- Les objets sélectionnés sont exportés dans un nouveau journal.
- Il s'agit de l'étape la plus importante de toute la procédure : ouvrez le nouveau journal et remplacez l'attribut + par - pour tous les objets que vous souhaitez supprimer. Assurez-vous que vous n'avez sélectionné aucun fichier/objet important du système d'exploitation.
- Ouvrez ESET SysInspector, cliquez sur **Fichier** > **Exécuter le script de services** entrez le chemin d'accès de votre script.
- Cliquez sur **OK** pour lancer le script.

4.7.4.1 Création d'un script de service

Pour créer un script, cliquez avec le bouton droit de la souris sur n'importe quel élément de l'arborescence de menus (dans le volet de gauche) dans la fenêtre principale de ESET SysInspector. Dans le menu contextuel, choisissez l'option **Exporter toutes les sections dans un script de service** ou **Exporter les sections sélectionnées dans un script de service**.

REMARQUE : il est impossible d'exporter le script de service lorsque deux journaux sont comparés.

4.7.4.2 Structure du script de service

La première ligne de l'en-tête du script reprend des informations sur la version du moteur (ev), la version de l'interface utilisateur graphique (gv) et la version du journal (lv). Ces données permettent d'identifier d'éventuelles modifications dans le fichier .xml qui génère le script et d'éviter toute incohérence durant l'exécution. Cette partie du script ne peut pas être modifiée.

Le reste du fichier est scindé en sections dont les éléments peuvent être modifiés (elles indiquent les éléments qui sont traités par le script). Pour marquer un élément à traiter, remplacez le caractère « - » qui le précède par « + ». Les sections du script sont séparées par une ligne vide. Chaque section possède un numéro et un titre.

01) Running processes (processus en cours)

Cette section contient la liste de tous les processus en cours d'exécution dans le système. Chaque processus est identifié par son chemin UNC, puis par son code de hachage CRC16 entre astérisques (*).

Exemple :

```
01) Running processes:
- \SystemRoot\System32\smss.exe *4725*
- C:\Windows\system32\svchost.exe *FD08*
+ C:\Windows\system32\module32.exe *CF8A*
[...]
```

Dans cet exemple, un processus, à savoir module32.exe, a été sélectionné (marqué par le caractère « + ») ; le processus s'arrête à l'exécution du script.

02) Loaded modules (modules chargés)

Cette section répertorie la liste des modules système en cours d'utilisation :

Exemple :

```
02) Loaded modules:
- c:\windows\system32\svchost.exe
- c:\windows\system32\kernel32.dll
+ c:\windows\system32\khbekhb.dll
- c:\windows\system32\advapi32.dll
[...]
```

Dans cet exemple, le module khbekhb.dll a été marqué par un « + ». Quand le script est exécuté, il reconnaît les processus qui utilisent ce module et les arrête.

03) TCP connections (connexions TCP)

Cette section contient des informations sur les connexions TCP existantes.

Exemple :

```
03) TCP connections:
- Active connection: 127.0.0.1:30606 -> 127.0.0.1:55320, owner: ekrn.exe
- Active connection: 127.0.0.1:50007 -> 127.0.0.1:50006,
- Active connection: 127.0.0.1:55320 -> 127.0.0.1:30606, owner: OUTLOOK.EXE
- Listening on *, port 135 (epmap), owner: svchost.exe
+ Listening on *, port 2401, owner: fservice.exe Listening on *, port 445 (microsoft-ds), owner: System
[...]
```

Lorsque le script est exécuté, il localise le propriétaire du socket dans les connexions TCP marquées et arrête le socket, ce qui libère des ressources système.

04) UDP endpoints (points de terminaison UDP)

Cette section contient des informations sur les points de terminaison UDP existants.

Exemple :

```
04) UDP endpoints:
- 0.0.0.0, port 123 (ntp)
+ 0.0.0.0, port 3702
- 0.0.0.0, port 4500 (ipsec-msft)
- 0.0.0.0, port 500 (isakmp)
[...]
```

Lorsque le script est exécuté, il isole le propriétaire du socket aux points de terminaison UDP marqués et arrête le socket.

05) DNS server entries (entrées du serveur DNS)

Cette section contient des informations sur la configuration actuelle du serveur DNS.

Exemple :

```
05) DNS server entries:
+ 204.74.105.85
- 172.16.152.2
[...]
```

Les entrées du serveur DNS marquées sont supprimées à l'exécution du script.

06) Important registry entries (entrées de Registre importantes)

Cette section contient des informations relatives aux entrées de Registre importantes.

Exemple :

```
06) Important registry entries:
* Category: Standard Autostart (3 items)
 HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- HotKeysCmds = C:\Windows\system32\hkcmd.exe
- IgfxTray = C:\Windows\system32\igfxtray.exe
 HKCU\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
- Google Update = "C:\Users\antoniak\AppData\Local\Google\Update\GoogleUpdate.exe" /c
* Category: Internet Explorer (7 items)
 HKLM\Software\Microsoft\Internet Explorer\Main
+ Default_Page_URL = http://thatcrack.com/
[...]
```

Les entrées marquées sont supprimées, réduites à des valeurs de 0 octet ou réinitialisées sur leur valeur par défaut lors de l'exécution du script. L'action à appliquer à chaque entrée dépend de la catégorie de l'entrée et de la valeur de la clé dans ce Registre.

07) Services (services)

Cette section répertorie les services enregistrés dans le système.

Exemple :

```
07) Services:
- Name: Andrea ADI Filters Service, exe path: c:\windows\system32\aeadisrv.exe, state: Running, startup:
Automatic
- Name: Application Experience Service, exe path: c:\windows\system32\aelupsvc.dll, state: Running, startup:
Automatic
- Name: Application Layer Gateway Service, exe path: c:\windows\system32\alg.exe, state: Stopped, startup:
Manual
[...]
```

Les services marqués et les services dépendants sont arrêtés et désinstallés après l'exécution du script.

08) Drivers (pilotes)

Cette section répertorie les pilotes installés.

Exemple :

```
08) Drivers:
- Name: Microsoft ACPI Driver, exe path: c:\windows\system32\drivers\acpi.sys, state: Running, startup: Boot
- Name: ADI UAA Function Driver for High Definition Audio Service, exe path: c:\windows\system32
\drivers\adihdaud.sys, state: Running, startup: Manual
[...]
```

Lorsque vous exécutez le script, les pilotes sélectionnés sont arrêtés. Notez que certains pilotes n'autoriseront pas leur arrêt.

09) Critical files (fichiers critiques)

Cette section contient des informations sur les fichiers essentiels au système d'exploitation.

Exemple :

```
09) Critical files:
* File: win.ini
- [fonts]
- [extensions]
- [files]
- MAPI=1
[...]
* File: system.ini
- [386Enh]
- woafont=dosapp.fon
- EGA80WOA.FON=EGA80WOA.FON
[...]
* File: hosts
- 127.0.0.1 localhost
- ::1 localhost
[...]
```

Les éléments sélectionnés sont soit supprimés, soit restaurés sur leur valeur d'origine.

4.7.4.3 Exécution des scripts de services

Marquez tous les éléments souhaités, puis enregistrez et fermez le script. Exécutez le script modifié directement depuis la fenêtre principale ESET SysInspector en choisissant l'option **Exécuter le script de services** dans le menu Fichier. Lorsque vous ouvrez un script, le programme affiche le message suivant : **Voulez-vous vraiment exécuter le script de service « %Scriptname% » ?** Une fois que vous avez confirmé votre sélection, un autre avertissement peut apparaître pour vous indiquer que le script de service que vous essayez d'exécuter n'a pas été signé. Cliquez sur **Exécuter** pour lancer le script.

Une boîte de dialogue confirmera l'exécution du script.

Si le script n'a pu être traité que partiellement, une boîte de dialogue avec le message suivant apparaît : **Le script de service n'a été exécuté que partiellement. Voulez-vous afficher le rapport d'erreurs ?** Choisissez **Oui** pour afficher un rapport des erreurs complexe qui répertorie les opérations qui n'ont pas été exécutées.

Si le script n'a pas été reconnu, une boîte de dialogue apparaîtra avec le message suivant : **Le script de service sélectionné n'est pas signé. L'exécution de scripts non signés et inconnus peut endommager gravement les données de votre ordinateur. Voulez-vous vraiment exécuter le script et ses actions ?** Ceci peut être le résultat d'incohérences au sein du script (en-tête endommagé, titre de section endommagé, ligne vide manquante entre les sections, etc.). Vous pouvez soit rouvrir le fichier de script et corriger les erreurs qu'il contient, soit créer un autre script de service.

4.7.5 FAQ

L'exécution d'ESET SysInspector requiert-elle des privilèges d'administrateur ?

Bien que ESET SysInspector puisse être exécuté sans privilèges d'administrateur, certaines des informations qu'il recueille peuvent être consultées uniquement via un compte administrateur. Une exécution en tant qu'utilisateur standard ou utilisateur disposant d'un accès restreint entraîne la collecte d'un volume inférieur d'informations sur l'environnement d'exploitation.

ESET SysInspector crée-t-il un fichier journal ?

ESET SysInspector peut créer un fichier journal sur la configuration de votre ordinateur. Pour en enregistrer un, dans le menu principal, sélectionnez **Fichier** > **Enregistrer le journal**. Les journaux sont enregistrés au format XML. Par défaut, les fichiers sont enregistrés dans le répertoire *%USERPROFILE%\Mes documents*, conformément à la convention de dénomination de fichier SysInspector-%COMPUTERNAME%-YYMMDD-HHMM.XML. Vos pouvez changer l'emplacement et le nom du fichier avant la sauvegarde si vous le souhaitez.

Comment puis-je consulter le fichier journal d'ESET SysInspector ?

Pour consulter un fichier journal créé par ESET SysInspector, exécutez le programme et choisissez **Fichier** > **Ouvrir le journal** dans le menu principal. Vous pouvez également faire glisser les fichiers journaux et les déposer sur l'application ESET SysInspector. Si vous devez consulter fréquemment les fichiers journaux ESET SysInspector, il est conseillé de créer un raccourci vers le fichier SYSINSPECTOR.exe sur le Bureau ; vous pourrez ensuite faire glisser les fichiers et les déposer sur ce raccourci. Pour des raisons de sécurité, Windows Vista/7 peuvent désactiver la fonction glisser-déposer entre des fenêtres dont les autorisations diffèrent.

Existe-t-il une spécification pour le format de fichier journal ? Existe-t-il un kit de développement logiciel (SDK) ?

Pour l'instant, il n'existe ni spécifications pour le fichier journal, ni SDK car le programme en est toujours au stade du développement. Après la diffusion du programme, nous fournirons ces éléments sur la base des commentaires et des demandes des clients.

Comment ESET SysInspector évalue-t-il le risque que pose un objet en particulier ?

Dans la majorité des cas, ESET SysInspector attribue des niveaux de risque aux objets (fichiers, processus, clés de Registre, etc.) sur la base d'une série de règles heuristiques qui examinent les caractéristiques de chaque objet, puis qui évaluent le potentiel d'activité malveillante. Sur la base de cette heuristique, un niveau de risque de 1 - Bon (vert) à 9 - Risqué (rouge) est attribué aux objets. Dans le volet de navigation gauche, la couleur des sections est définie par le niveau de risque le plus élevé d'un des objets qu'elles contiennent.

Un niveau de risque « 6 - Inconnu (rouge) » signifie-t-il que l'objet est dangereux ?

Les évaluations d'ESET SysInspector ne garantissent pas qu'un objet est malveillant. Cette réponse doit être apportée par l'expert en sécurité. ESET SysInspector a été développé pour fournir aux experts en sécurité une évaluation rapide afin qu'ils puissent identifier les objets d'un système qui doivent faire l'objet d'un examen plus approfondi en cas de comportement étrange.

Pourquoi ESET SysInspector se connecte-t-il à Internet ?

À l'instar de nombreuses applications, ESET SysInspector possède un « certificat » avec une signature numérique qui permet de garantir que le logiciel a bien été diffusé par ESET et qu'il n'a pas été modifié. Afin de vérifier le certificat, le système d'exploitation contacte une autorité de certification pour confirmer l'identité de l'éditeur de logiciels. Il s'agit d'un comportement normal pour tous les programmes avec signature numérique sous Microsoft Windows.

Qu'est-ce que la technologie Anti-Stealth ?

La technologie Anti-Stealth offre une détection efficace des rootkits.

Quand un système est attaqué par un code malveillant qui se comporte comme un rootkit, l'utilisateur risque une perte ou un vol de données. Sans outil spécial de lutte contre les rootkits, il est pratiquement impossible de les détecter.

Pourquoi y a-t-il parfois des fichiers marqués comme « Signé par MS » avec une valeur différente dans le champ « Nom de la société » ?

Lorsqu'il tente d'identifier la signature numérique d'un fichier exécutable, ESET SysInspector recherche d'abord une signature numérique intégrée au fichier. Si une signature numérique est détectée, le fichier est validaté à l'aide de ces informations. En revanche, si aucune signature numérique n'est détectée, ESI lance la recherche du fichier CAT correspondant (Catalogue de sécurité - *%systemroot%\system32\catroot*) qui contient les informations relatives au fichier exécutable traité. Si le fichier CAT pertinent est trouvé, la signature numérique du fichier CAT est appliquée dans la procédure de validation du fichier exécutable.

Voilà pourquoi des fichiers sont parfois marqués « Signé par MS » mais ont un « Nom de la société » différent.

Exemple :

Windows 2000 comprend l'application HyperTerminal qui se trouve dans *C:\Program Files\Windows NT*. Le fichier exécutable principal de l'application n'a pas de signature numérique, mais ESET SysInspector l'indique comme étant un fichier signé par Microsoft. Ceci s'explique par une référence dans *C:\WINNT\system32\CatRoot\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\sp4.cat* qui pointe vers *C:\Program Files\Windows NT\hypertrm.exe* (le fichier exécutable principal de l'application HyperTerminal) et *sp4.cat* qui possède une signature numérique de Microsoft.

4.7.6 ESET SysInspector en tant que partie de ESET File Security

Pour ouvrir la section ESET SysInspector de ESET File Security, cliquez sur **Outils** > **ESET SysInspector**. Le système de gestion de la fenêtre ESET SysInspector est semblable à celui des journaux d'analyse des ordinateurs ou des tâches planifiées. Toutes les opérations effectuées avec des instantanés système (création, affichage, comparaison, suppression et exportation) sont accessibles en un ou deux clics.

La fenêtre ESET SysInspector contient les informations élémentaires concernant les instantanés créés : heure de création, bref commentaire, nom de l'utilisateur auteur de l'instantané et statut de l'instantané.

Pour comparer, créer ou supprimer des instantanés, utilisez les boutons correspondants situés en dessous de la liste des instantanés dans la fenêtre ESET SysInspector. Ces options sont également disponibles dans le menu contextuel. Pour afficher l'instantané du système sélectionné, utilisez l'option **Afficher** du menu contextuel. Pour exporter l'instantané sélectionné dans un fichier, cliquez dessus avec le bouton droit de la souris et sélectionnez **Exporter...**

Voici la description détaillée des options disponibles :

- **Comparer** - permet de comparer deux journaux. Elle est particulièrement adaptée si vous souhaitez effectuer le suivi des modifications entre le journal actuel et un ancien journal. Pour que cette option entre en vigueur, vous devez sélectionner deux instantanés à comparer.
- **Créer...** - Crée un enregistrement. Au préalable, vous devez entrer un bref commentaire sur l'enregistrement. Pour consulter le pourcentage de progression de la création de l'instantané en cours, consultez la colonne **Statut**. Tous les instantanés terminés ont le statut **Créé**.
- **Effacer/Effacer tout** - Supprime les entrés de la liste.
- **Exporter...** - Cette option enregistre l'entrée sélectionnée dans un fichier XML (également dans une version compressée).

4.8 ESET SysRescue

ESET SysRescue est un utilitaire qui vous permet de créer un disque amorçable contenant une des solutions ESET Security - il peut s'agir de ESET NOD32 Antivirus, ESET Smart Security, ou d'un des produits orientés serveur. Le principal avantage de ESET SysRescue réside dans le fait que la solution ESET Security s'exécute indépendamment du système d'exploitation hôte, tout en ayant un accès direct au disque et à l'ensemble du système de fichiers. Il est par conséquent possible de supprimer les infiltrations qui ne pourraient normalement pas être supprimées, par exemple lorsque le système d'exploitation est en cours d'exécution.

4.8.1 Configuration minimale requise

ESET SysRescue fonctionne dans l'environnement de préinstallation Microsoft Windows (Windows PE) version 2.x basé sur Windows Vista.

Windows PE fait partie du Kit d'installation automatisée de Windows (Windows AIK) ou du Kit d'évaluation et de déploiement de Windows (Windows ADK). Windows AIK ou ADK doit donc être installé avant la création d'ESET SysRescue (http://go.eset.eu/AIK) ou (http://go.eset.eu/ADK). Le kit à installer sur votre système dépend de la version du système d'exploitation utilisé. Windows PE prenant en charge la version 32 bits, le package d'installation d'ESET Security 32 bits doit être installé lors de la création d'ESET SysRescue sur des systèmes 64 bits. ESET SysRescue prend en charge Windows AIK 1.1 et versions ultérieures, ainsi que Windows ADK.

REMARQUE : Étant donné que la taille de Windows AIK est de plus de 1 Go et celle de Windows ADK de 1,3 GO, une connexion Internet rapide est nécessaire pour un téléchargement efficace.

ESET SysRescue est disponible dans les ESET Security version 4.0 et suivantes.

ESET SysRescue prend en charge les systèmes d'exploitation suivants :

- Windows Server 2003 Service Pack 1 avec KB926044
- Windows Server 2003 Service Pack 2
- Windows Server 2008
- Windows Server 2012

Windows AIK prend en charge :

- Windows Server 2003
- Windows Server 2008

Windows ADK prend en charge :

- Windows Server 2012

4.8.2 Procédure de création d'un CD de dépannage

Pour lancer l'Assistant ESET SysRescue, cliquez sur **Démarrer** > **Programmes** > **ESET** > **ESET File Security** > **ESET SysRescue**.

Tout d'abord, l'Assistant vérifie si Windows AIK ou Windows ADK est installé et si un périphérique adapté pour la création du support d'amorçage est présent. Si Windows AIK ou Windows ADK n'est pas installé sur l'ordinateur (ou si l'installation est endommagée ou incorrecte), l'Assistant vous propose de l'installer ou de saisir le chemin d'accès à votre dossier Windows AIK (http://go.eset.eu/AIK) ou Windows ADK (http://go.eset.eu/ADK).

REMARQUE : Étant donné que la taille de Windows AIK est de plus de 1 Go et celle de Windows ADK de 1,3 GO, une connexion Internet rapide est nécessaire pour un téléchargement efficace.

Au cours de l'étape suivante, sélectionnez le support cible où ESET SysRescue est créé.

4.8.3 Sélection de la cible

Outre la sauvegarde sur un CD/DVD/périphérique USB, vous pouvez enregistrer ESET SysRescue dans un fichier ISO. Ensuite, vous pouvez graver l'image ISO sur un CD/DVD, ou l'utiliser d'une autre manière (dans un environnement virtuel tel que VmWare ou Virtualbox par exemple).

Si vous choisissez USB en tant que support cible, le démarrage peut ne pas fonctionner sur certains ordinateurs. Certaines versions du BIOS peuvent signaler des problèmes de communication entre le BIOS et le gestionnaire de démarrage (par exemple sous Windows Vista) et le démarrage s'arrête sur l'erreur suivante :

```
file : \boot\bcd
status : 0xc000000e
info : an error occurred while attemping to read the boot configuration data (une erreur s'est produite pendant la ten
```

Si ce message s'affiche, il est conseillé de sélectionner CD au lieu d'USB en tant que support.

4.8.4 Paramètres

Avant de commencer la création d'ESET SysRescue, l'Assistant d'installation affiche les paramètres de compilation à la dernière étape de l'assistant ESET SysRescue. Cliquez pour ce faire sur le bouton **Changer...** Les options disponibles sont les suivantes :

- Dossiers
- ESET Antivirus
- Paramètres avancés
- Protocole Internet
- Périphérique USB amorçable (lorsque le périphérique USB cible est sélectionné)
- Gravure (lorsque le CD/DVD cible est sélectionné)

Le bouton **Créer** est inactif si aucun package d'installation MSI n'a été défini ou si aucune solution ESET Security n'est installée sur l'ordinateur. Pour sélectionner un package d'installation, cliquez sur le bouton **Modifier**, puis accédez à l'onglet **Antivirus ESET**. Si vous ne saisissez pas le nom d'utilisateur et le mot de passe (**Modifier** > **Antivirus ESET**), le bouton **Créer** est inactif.

4.8.4.1 Dossiers

Le **dossier temporaire** est un dossier de travail dans lequel sont stockés les fichiers nécessaires à la compilation d'ESET SysRescue.

Le **dossier ISO** est un dossier dans lequel est enregistré le fichier ISO après la compilation.

La liste dans cet onglet répertorie tous les disques de réseau locaux et mappés, ainsi que l'espace disponible. Si certains des dossiers sont stockés sur un lecteur ne disposant pas de l'espace suffisant, il est conseillé de sélectionner un autre lecteur avec plus d'espace disponible. Dans le cas contraire, la compilation pourrait s'arrêter prématurément en raison d'un manque d'espace sur le disque.

Applications externes : vous permet d'indiquer des programmes supplémentaires qui seront exécutés ou installés après l'amorçage depuis un support ESET SysRescue.

Inclure les applications externes : permet d'ajouter des programmes externes à la compilation ESET SysRescue.

Dossier sélectionné : dossier dans lequel se trouvent les programmes à ajouter au disque ESET SysRescue.

4.8.4.2 ESET Antivirus

Pour créer le CD ESET SysRescue, vous pouvez sélectionner deux sources de fichiers ESET à utiliser par le compilateur.

Dossier ESS/EAV : fichiers déjà contenus dans le dossier dans lequel la solution ESET Security est installée sur l'ordinateur.

Fichier MSI : les fichiers contenus dans le programme d'installation MSI sont utilisés.

Vous pouvez choisir de mettre à jour l'emplacement des fichiers (.nup). Normalement, l'option par défaut **Dossier ESS/EAV/Fichier MSI** doit être définie. Dans certains cas, il est possible de choisir un **dossier de mise à jour**, par exemple pour utiliser une version de base des signatures de virus plus ancienne ou plus récente.

Vous pouvez utiliser l'une des deux sources suivantes pour le nom d'utilisateur et le mot de passe :

ESS/EAV installé - Le nom d'utilisateur et le mot de passe sont copiés depuis la version installée de la solution ESET Security.

De l'utilisateur - Le nom d'utilisateur et le mot de passe saisis dans les zones de texte correspondantes sont utilisés.

REMARQUE : La solution ESET Security sur le CD ESET SysRescue est mise à jour soit via Internet, soit par l'intermédiaire de la solution ESET Security installée sur l'ordinateur sur lequel le CD ESET SysRescue est exécuté.

4.8.4.3 Paramètres avancés

L'onglet **Avancé** permet d'optimiser le CD ESET SysRescue en fonction de la quantité de mémoire disponible sur l'ordinateur. Sélectionnez **576 Mo et plus** pour écrire le contenu du CD dans la mémoire vive (RAM). Si vous choisissez **moins de 576 Mo**, l'accès au CD de récupération aura lieu en permanence lorsque WinPE est en exécution.

Dans la section **Pilotes externes**, vous pouvez installer les pilotes de votre matériel (en général, une carte de réseau). Bien que WinPE repose sur Windows Vista PS1 qui prend en charge une large gamme de matériel, il arrive parfois que le matériel ne soit pas reconnu. Dans ce cas, un pilote doit être ajouté manuellement. L'installation du pilote dans la compilation ESET SysRescue peut s'effectuer de deux manières : manuellement (à l'aide du bouton **Ajouter**) et automatiquement (par l'intermédiaire du bouton **Recherche auto**). En cas d'installation manuelle, vous devez choisir le chemin d'accès au fichier .inf correspondant (le fichier *.sys applicable doit se trouver également dans le dossier). En cas d'installation automatique, le pilote est détecté automatiquement dans le système d'exploitation de l'ordinateur. Il est conseillé d'utiliser l'introduction automatique uniquement si ESET SysRescue est utilisé sur un ordinateur qui possède la même carte de réseau que l'ordinateur sur lequel le CD ESET SysRescue a été créé. Lors de la création d'ESET SysRescue, le pilote est installé dans la compilation, ce qui évite à l'utilisateur d'avoir à le rechercher ultérieurement.

4.8.4.4 Protocole Internet

Cette section vous permet de configurer les informations réseau de base et de définir les connexions prédéfinies en fonction d'ESET SysRescue.

Sélectionnez **Adresse IP privée automatique** pour obtenir l'adresse IP automatiquement depuis le serveur DHCP (Dynamic Host Configuration Protocol).

Cette connexion réseau peut également utiliser une adresse IP spécifiée manuellement (appelée également adresse IP statique). Sélectionnez **Personnalisé** pour configurer les paramètres IP appropriés. Si vous sélectionnez cette option, vous devez indiquer une **adresse IP** et, pour les connexions Internet grande vitesse, un **masque de sous-réseau**. Dans **Serveur DNS préféré** et **Serveur DNS de rechange**, saisissez les adresses principale et secondaire de serveur DNS.

4.8.4.5 Périphérique USB d'amorçage

Si vous avez choisi le périphérique USB en tant que support cible, vous pouvez choisir l'un des périphériques USB disponibles dans l'onglet **Périphérique USB d'amorçage** (si plusieurs périphériques USB existent).

Sélectionnez le **périphérique** cible approprié sur lequel ESET SysRescue va être installé.

Avertissement : le périphérique USB sélectionné est formaté lors de la création d'ESET SysRescue. Toutes les données du périphérique sont supprimées.

Si vous choisissez l'option **Format rapide**, le formatage supprime tous les fichiers de la partition, mais ne recherche pas les secteurs endommagés du disque. Utilisez cette option si votre périphérique USB a été déjà formaté et que vous êtes certain qu'il n'est pas endommagé.

4.8.4.6 Graver

Si vous avez choisi CD/DVD en tant que support cible, vous pouvez définir les paramètres de gravure complémentaires dans l'onglet **Graver**.

Supprimer fichier ISO - Cochez cette case pour supprimer le fichier ISO temporaire après la création du CD ESET SysRescue.

Suppression activée - Permet de choisir entre la suppression rapide et la suppression complète.

Graveur - Choisissez le lecteur à utiliser pour la gravure.

Avertissement : il s'agit de l'option par défaut. En cas d'utilisation d'un CD/DVD réinscriptible, toutes les données sur le CD/DVD sont supprimées.

La section Support contient des informations sur le support dans le lecteur de CD/DVD.

Vitesse de gravure : sélectionnez la vitesse souhaitée dans le menu déroulant. Les capacités du périphérique de gravure et le type de CD/DVD utilisé doivent être pris en compte lors de la sélection de la vitesse de gravure.

4.8.5 Utilisation d'ESET SysRescue

Pour que le CD/DVD/USB de récupération fonctionne efficacement, l'ordinateur doit être démarré depuis le support d'amorçage ESET SysRescue. La priorité d'amorçage peut être modifiée dans le BIOS. Vous pouvez également utiliser le menu d'amorçage au démarrage de l'ordinateur (généralement à l'aide de l'une des touches F9 à F12) en fonction de la version de la carte mère ou du BIOS.

Une fois l'amorçage depuis le support d'amorçage terminé, la solution ESET Security démarre. Comme ESET SysRescue n'est utilisé que dans des situations spécifiques, certains modules de protection et fonctionnalités de programme présents dans la version standard de ESET Security ne sont pas nécessaires ; leur liste est limitée à l' **Analyse de l'ordinateur**, à la **Mise à jour** et à certaines sections de la **Configuration**. ESET SysRescue peut mettre à jour la base des signatures de virus. C'est la principale fonctionnalité de cette application et nous vous recommandons d'effectuer cette mise à jour avant de lancer l'analyse de l'ordinateur.

4.8.5.1 Utilisation d'ESET SysRescue

En supposant que des ordinateurs du réseau aient été infectés par un virus modifiant des fichiers exécutables (.exe). La solution ESET Security est capable de nettoyer tous les fichiers infectés, à l'exception d'*explorer.exe* qui ne peut pas être nettoyé, même en mode sans échec. Cela est dû au fait que le fichier *explorer.exe*, c'est-à-dire l'un des principaux processus de Windows, est également lancé en mode sans échec. La solution ESET Security n'exécute aucune opération et le fichier reste infecté.

Dans ce type de scénario, vous pouvez utiliser ESET SysRescue pour résoudre le problème. ESET SysRescue ne requiert aucun composant du système d'exploitation hôte et peut traiter (nettoyer, supprimer) n'importe quel fichier sur le disque.

4.9 Interface utilisateur

La configuration de l'interface utilisateur d'ESET File Security peut être modifiée de manière à pouvoir ajuster l'environnement de travail selon vos besoins. Ces options de configuration sont accessibles depuis la branche **Interface utilisateur** de l'arborescence de configuration avancée de ESET File Security.

Dans la section **Éléments de l'interface utilisateur**, l'option **Mode avancé** permet aux utilisateurs de passer au mode avancé. Le mode avancé affiche des paramètres détaillés et des commandes supplémentaires pour ESET File Security.

L'**interface utilisateur graphique** doit être désactivée si les éléments graphiques ralentissent les performances de l'ordinateur ou causent d'autres problèmes. De la même manière, il est peut-être nécessaire de désactiver l'interface utilisateur graphique pour les utilisateurs malvoyants, car elle peut créer un conflit avec des applications spéciales utilisées pour la lecture de textes affichés à l'écran.

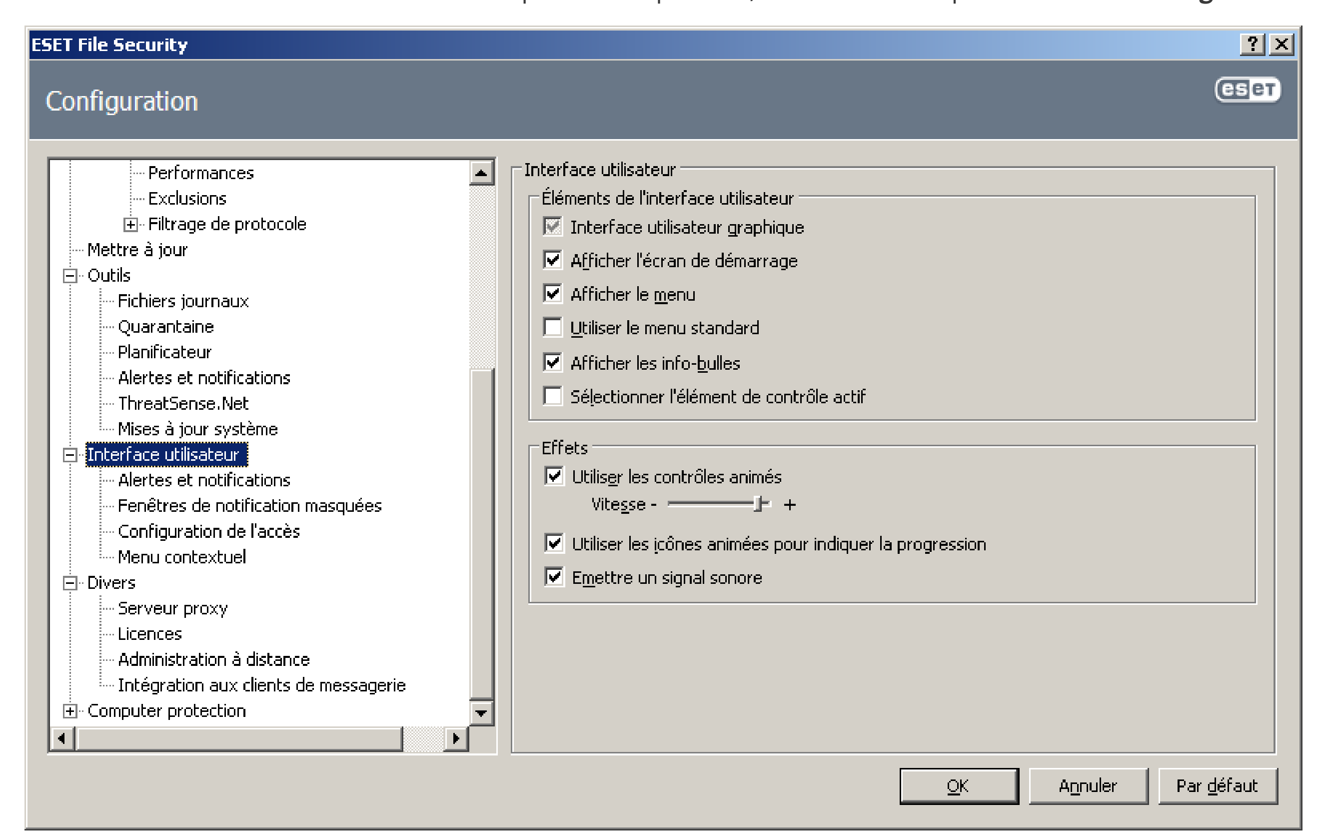
Pour désactiver l'écran de démarrage de ESET File Security, désélectionnez l'option **Afficher l'écran de démarrage**.

En haut de la fenêtre principale de programme de ESET File Security figure un menu standard qui peut être activé ou désactivé en fonction de l'option **Utiliser le menu standard**.

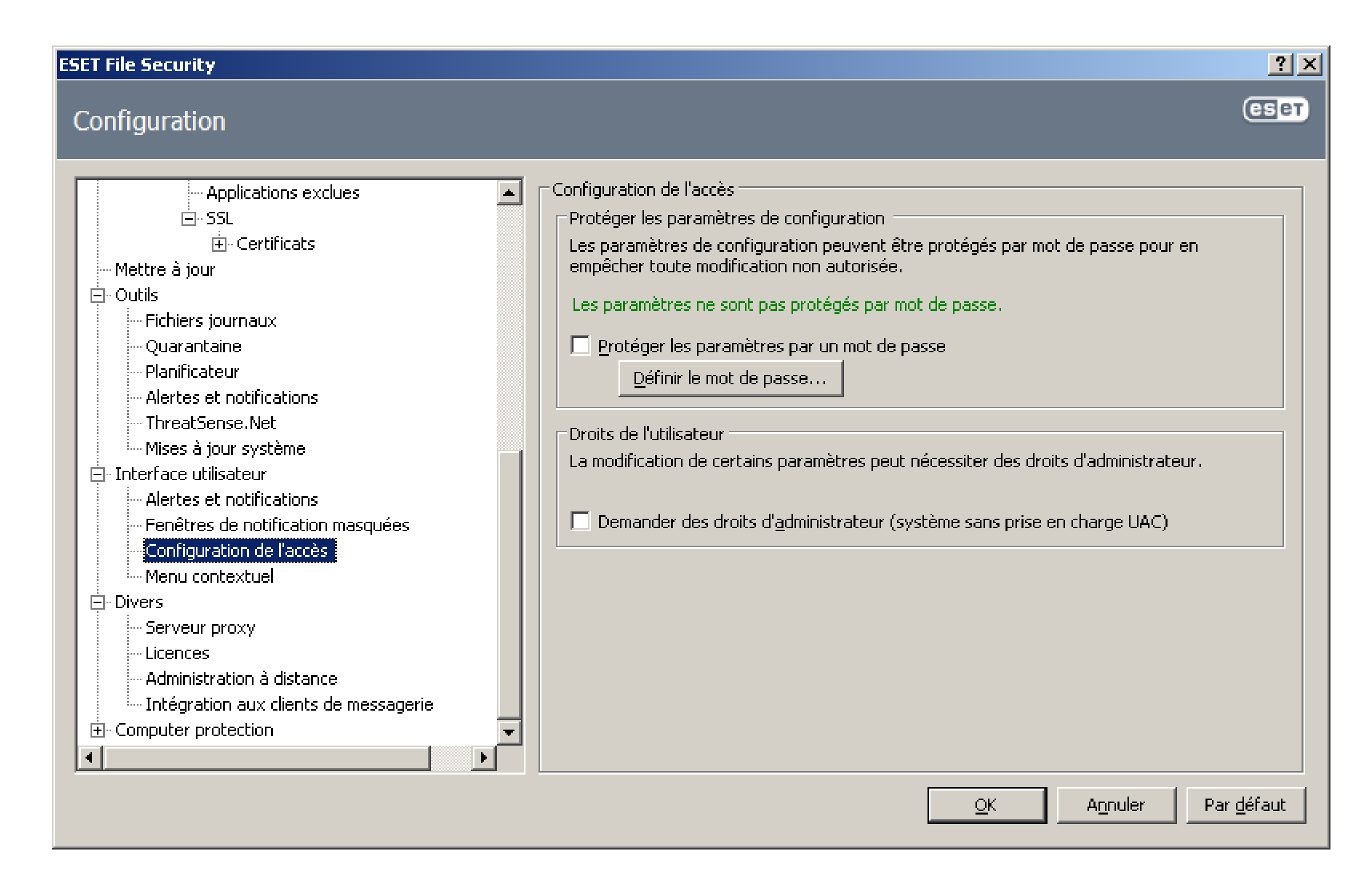
Si l'option **Afficher les info-bulles** est activée, une courte description apparaît si le curseur est immobilisé sur une option. Lorsque l'option **Sélectionner l'élément de contrôle actif** est sélectionnée, le système met en évidence tout élément situé dans la zone active du curseur de la souris. L'élément mis en évidence est activé si l'utilisateur clique dessus.

Pour diminuer ou augmenter la vitesse des effets animés, sélectionnez l'option **Utiliser les contrôles animés** et déplacez le curseur **Vitesse** vers la gauche ou vers la droite.

Pour activer l'utilisation des icônes animées afin d'afficher la progression des différentes opérations, sélectionnez l'option **Utiliser les icônes animées pour indiquer la progression**. Si vous souhaitez que le programme émette un son d'avertissement si un événement important se produit, sélectionnez l'option **Émettre un signal sonore**.



Les fonctionnalités d'**interface utilisateur** permettent également de protéger les paramètres de configuration de ESET File Security par mot de passe. Cette option se trouve dans le sous-menu **Protection des paramètres** dans **Interface utilisateur**. Il est essentiel que le programme soit correctement configuré pour garantir le maximum de sécurité au système. Tout changement non autorisé peut provoquer la perte de données importantes. Pour définir un mot de passe visant à protéger les paramètres de configuration, cliquez sur **Définir le mot de passe...**



4.9.1 Alertes et notifications

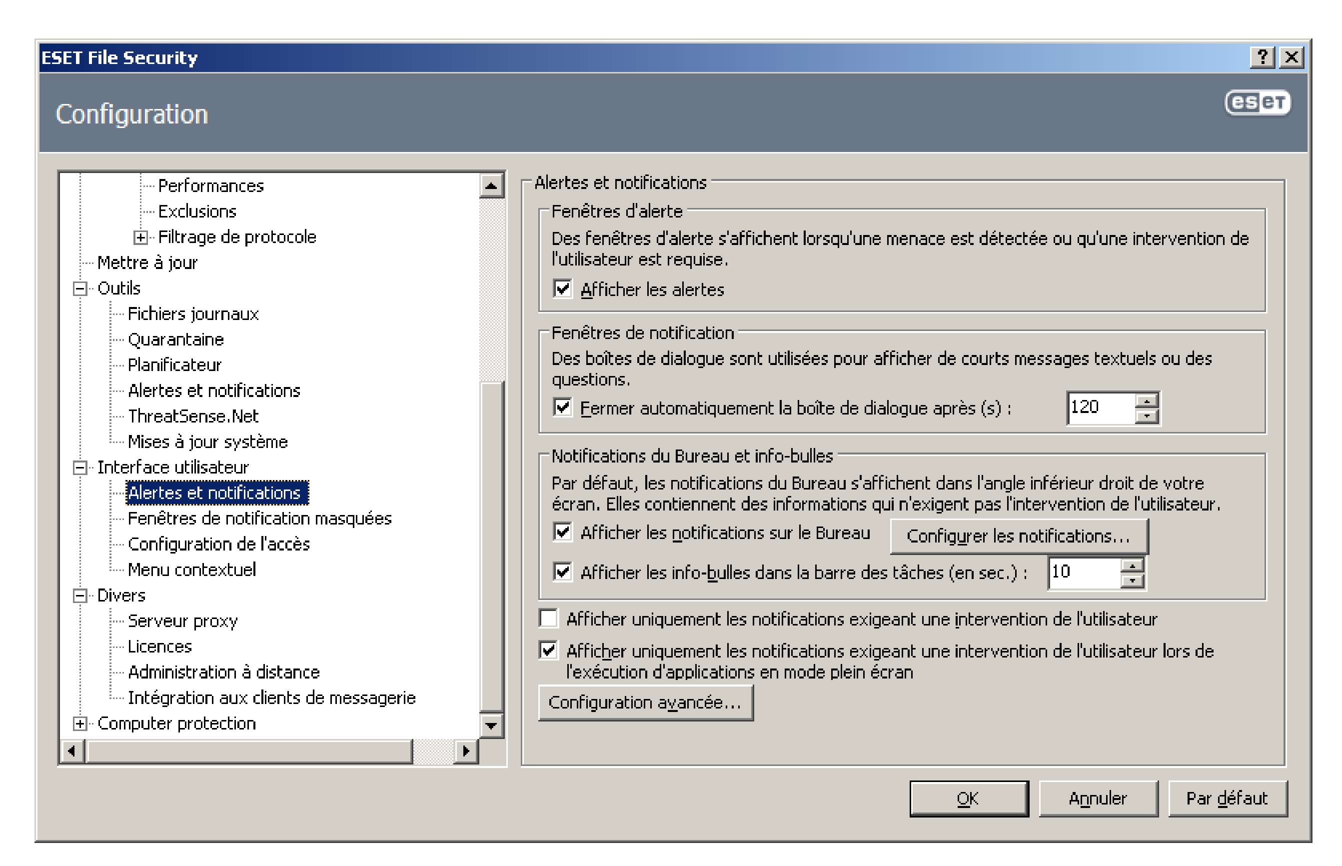
La section **Configurer les alertes et notifications** dans **Interface utilisateur** vous permet de configurer le mode de traitement des alertes en cas de menace et des notifications système dans ESET File Security.

La première option est **Afficher les alertes**. Lorsqu'elle est désactivée, aucune fenêtre d'alerte ne s'affiche, ce qui ne convient qu'à un nombre limité de situations particulières. Nous recommandons à la majorité des utilisateurs de conserver l'option par défaut (activée).

Pour fermer automatiquement les fenêtres d'alerte après un certain délai, sélectionnez l'option **Fermer automatiquement la boîte de dialogue après (s)**. Si les fenêtres d'alerte ne sont pas fermées manuellement, le système les ferme automatiquement une fois le laps de temps écoulé.

Les notifications sur le bureau et les infobulles sont fournies à titre d'information uniquement et ne permettent ni n'exigent aucune interaction avec l'utilisateur. Elles s'affichent dans la partie système de la barre d'état, dans l'angle inférieur droit de l'écran. Pour activer l'affichage des notifications sur le bureau, activez l'option **Afficher les notifications sur le bureau**. Vous pouvez modifier d'autres options détaillées (la durée d'affichage des notifications et la transparence de la fenêtre) en cliquant sur le bouton **Configurer les notifications...**

Pour prévisualiser le comportement des notifications, cliquez sur le bouton **Aperçu**. Pour configurer la durée d'affichage des infobulles, utilisez l'option **Afficher les infos-bulles dans la barre des tâches (s)**.



Cliquez sur **Configuration avancée...** pour indiquer des options de configuration supplémentaires **Alertes et notifications**, notamment l'option **Afficher uniquement les notifications exigeant une intervention de l'utilisateur**. Cette option vous permet d'activer/de désactiver l'affichage des alertes et des notifications qui n'exigent aucune interaction de l'utilisateur. Sélectionnez **Afficher uniquement les notifications exigeant une intervention de l'utilisateur lors de l'exécution d'applications en mode plein écran** pour supprimer toutes les notifications non interactives. Dans le menu déroulant **Verbosité minimale des événements à afficher**, vous pouvez sélectionner le niveau de gravité de démarrage des alertes et notifications à afficher.

La dernière fonctionnalité de cette section permet de configurer la destination des notifications dans un environnement multi-utilisateur. **Sur les systèmes multi-utilisateurs, afficher les notifications sur l'écran de l'utilisateur suivant** : permet de définir l'utilisateur qui recevra les notifications importantes d'ESET File Security. Normalement, il doit s'agir de l'administrateur système ou de l'administrateur réseau. Cette option est particulièrement utile pour les serveurs Terminal Server, pour autant que toutes les notifications système soient envoyées à l'administrateur.

4.9.2 Désactivation de l'interface utilisateur graphique sur Terminal Server

Ce chapitre indique comment désactiver l'interface utilisateur graphique d'ESET File Security sur Windows Terminal Server pour les sessions utilisateur.

Normalement, l'interface utilisateur graphique d'ESET File Security démarre chaque fois qu'un utilisateur distant se connecte au serveur et crée une session de terminal. Cet affichage n'est généralement pas conseillé sur les serveurs Terminal Server. Si vous souhaitez désactiver l'interface utilisateur graphique pour les sessions de terminal, procédez comme suit :

1. Exécutez *regedit.exe*
2. Accédez à *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run*
3. Cliquez avec le bouton droit sur la valeur *egui* et sélectionnez *Modifier...*
4. Ajoutez un paramètre `/terminal` à la fin d'une chaîne existante

Voici un exemple des données de valeur *egui* :

```
"C:\Program Files\ESET\ESET File Security\egui.exe" /hide /waitservice /terminal
```

Si vous souhaitez rétablir ce paramètre et activer le démarrage automatique de l'interface utilisateur graphique d'ESET File Security, supprimez le paramètre `/terminal` . Pour accéder à la valeur de registre *egui*, répétez les étapes 1 à 3.

4.10 eShell

eShell (abréviation d'ESET Shell) est une interface à ligne de commande pour ESET File Security. Il s'agit d'une alternative à l'interface graphique. eShell dispose de toutes les fonctionnalités et options que propose normalement l'interface graphique. eShell vous permet de configurer et administrer tout le programme sans utiliser l'interface graphique.

Outre les fonctions et fonctionnalités disponible dans l'interface graphique, l'interface à ligne de commande vous permet d'automatiser l'exécution de scripts afin de configurer et de modifier la configuration, ou encore d'effectuer une opération. eShell est également utile pour les utilisateurs qui préfèrent les lignes de commande aux interfaces graphiques.

Cette section indique comment parcourir et utiliser le système eShell. Elle répertorie également toutes les commandes et décrit chaque commande, ainsi que l'opération qu'elle effectue.

Le système eShell peut être exécuté de deux manières :

- Mode interactif : ce mode est utile lorsque vous souhaitez utiliser régulièrement eShell (pas simplement exécuter une seule commande), par exemple lorsque vous modifiez la configuration, affichez des journaux, etc. Vous pouvez également utiliser le mode interactif si vous ne connaissez pas encore toutes les commandes. Le mode interactif simplifie la navigation dans eShell. Il affiche également les commandes que vous pouvez utilisez dans un contexte défini.
- Commande unique/mode de traitement par lots : vous pouvez utiliser ce mode si vous avez uniquement besoin d'exécuter une commande sans passer au mode interactif de eShell. Pour ce faire, saisissez dans l'invite de commande Windows `eShell` et ajoutez les paramètres appropriés. Par exemple :

```
eshell set av document status enabled
```

REMARQUE : afin d'exécuter les commandes eShell depuis l'invite de commande Windows ou d'exécuter les fichiers en mode de traitement par lots, cette fonction doit d'abord être activée (la commande `set general access batch always` doit être exécutée en mode interactif). Pour plus d'informations sur la commande set batch, cliquez ici.

Pour passer au mode interactif eShell, vous pouvez utiliser l'une des deux méthodes suivantes :

- Par l'intermédiaire du menu Démarrer de Windows : **Démarrer** > **Tous les programmes** > **ESET** > **ESET File Security** > **ESET shell**
- Depuis l'invite de commande Windows en tapant `eShell` et en appuyant sur la touche Entrée.

Lorsque vous exécutez eShell en mode interactif pour la première fois, l'écran de première exécution s'affiche.

```
ESET Shell
ESET Shell 1.0
Copyright (c) 1992-2012 ESET, spol. s r. o. Tous droits réservés.
------------------------------------------------------------------------------
Première exécution
Pour afficher de nouveau ces informations, saisissez les informations
suivantes :
        guide      /?      -help

Syntaxe :
        [<préfixe>] [<chemin de commande>]  <commande> [<arguments>]

Par exemple, pour activer la protection des documents, saisissez les
informations suivantes :
            set          av document        status      enabled

Opération
La commande peut prendre en charge ou ne pas prendre en charge toutes les
opérations. Les opérations changent la signification de la commande. Par
exemple, get av status renvoie l'état de la protection antivirus tandis que set
av status enabled active cette protection. La commande exit est un exemple de
commande sans préfixe.

Les opérations disponibles sont les suivantes :
        get             set             select          add             remove
-- Autres -- (ENTRÉE - Ligne, ESPACE - Page, X - Fin)
```

Il présente des exemples de base concernant l'utilisation d'eShell avec une syntaxe, un préfixe, un chemin d'accès à une commande, des formes abrégées, des alias, etc. Il constitue un guide rapide d'utilisation d'eShell.

REMARQUE : Si vous souhaitez afficher ultérieurement cet écran de première exécution, tapez la commande `guide` .

REMARQUE : Les commandes ne font pas la distinction entre les majuscules et les minuscules : que vous saisissiez

les noms de commande en majuscules ou en minuscules, les commandes s'exécutent de la même manière.

4.10.1 Utilisation

Syntaxe
Pour qu'elles fonctionnent correctement, les commandes doivent avec une syntaxe correcte. Elles peuvent être composées d'un préfixe, d'un contexte, d'arguments, d'options, etc. Voici la syntaxe générale utilisée dans eShell :

[<préfixe>] [<chemin de la commande>] <commande> [<arguments>]

Exemple (cette commande active la protection des documents) :
```
SET AV DOCUMENT STATUS ENABLED
```

`SET` - préfixe
`AV DOCUMENT` - chemin vers une commande particulière, contexte auquel la commande appartient
`STATUS` - commande proprement dite
`ENABLED` - argument de la commande

L'utilisation de la valeur `HELP` ou `?` avec une commande affiche la syntaxe de cette commande. Par exemple, la commande `CLEANLEVEL HELP` affiche la syntaxe de la commande `CLEANLEVEL` :

SYNTAXE :
```
[get] | restore cleanlevel
set cleanlevel none | normal | strict
```

Vous pouvez constater que `[get]` est entre crochets. Cela indique que le préfixe `get` est l'option par défaut de la commande `cleanlevel` . En d'autres termes, lorsque vous exécutez la commande `cleanlevel` sans indiquer de préfixe, la commande utilise le préfixe par défaut (dans ce cas `get cleanlevel`). Vous gagnerez du temps en n'indiquant pas de préfixe. La valeur `get` est généralement le préfixe par défaut pour la plupart des commandes, mais vous devez effectuer cette vérification pour chaque commande et vous assurer qu'il correspond bien à l'instruction que vous souhaitez exécuter.

REMARQUE : Les commandes ne font pas la distinction entre les majuscules et les minuscules : que vous saisissiez les noms de commande en majuscules ou en minuscules, les commandes s'exécutent de la même manière.

Préfixe/Opération
Un préfixe est une opération. La commande `GET` fournit des informations sur la configuration d'une fonctionnalité de ESET File Security ou indique l'état (`GET AV STATUS` affiche l'état de la protection en cours). La commande `SET` (préfixe) configure la fonctionnalité ou change son état (`SET AV STATUS ENABLED` active la protection).

eShell vous permet d'utiliser ces préfixes. Les commandes peuvent prendre en charge ou ne pas prendre en charge les préfixes :

`GET` - renvoie le paramètre/l'état en cours.
`SET` - définit la valeur/l'état.
`SELECT` - sélectionne un élément.
`ADD` - ajoute un élément.
`REMOVE` - supprime un élément.
`CLEAR` - supprime tous les éléments/fichiers.
`START` - démarre une action.
`STOP` - arrête une action.
`PAUSE` - interrompt une action.
`RESUME` - reprend une action.
`RESTORE` - restaure les paramètres/l'objet/le fichier par défaut.
`SEND` - envoie un objet/fichier.
`IMPORT` - importe d'un fichier.
`EXPORT` - exporte dans un fichier.

Les préfixes tels que `GET` et `SET` sont utilisés avec de nombreuses commandes (certaines commandes telles que `EXIT`) n'utilisent pas de préfixe.

Chemin/Contexte de la commande
Les commandes sont placées dans des contextes qui constituent une arborescence. Le niveau supérieur de l'arborescence est la racine. Lorsque vous exécutez eShell, vous vous trouvez au niveau racine :

```
eShell>
```

Vous pouvez exécuter la commande depuis cet emplacement ou saisir le nom du contexte dans l'arborescence pour y accéder. Par exemple, lorsque vous saisissez le contexte TOOLS , toutes les commandes et sous-contextes disponibles depuis cet emplacement sont répertoriés.

```
ESET Shell
eShell>av
GET ANTISTEALTH      SET ANTISTEALTH      RESTORE ANTISTEALTH
GET CLEANLEVEL       SET CLEANLEVEL       RESTORE CLEANLEVEL
DOCUMENT             EMAIL                GET EXCLUSIONS
ADD EXCLUSIONS       REMOVE EXCLUSIONS    CLEAR EXCLUSIONS
GET EXTENSIONS       ADD EXTENSIONS       REMOVE EXTENSIONS
RESTORE EXTENSIONS   LIMITS               NETFILTER
OBJECTS              OPTIONS              OTHER
REALTIME             RESTART              GET SELFDEFENSE
SET SELFDEFENSE      RESTORE SELFDEFENSE  GET STATUS
SET STATUS           RESTORE STATUS       WEB

eShell av>_
```

Les éléments en jaune correspondent aux commandes que vous pouvez exécuter et les éléments en gris sont des sous-contextes que vous pouvez saisir. Un sous-contexte contient des commandes supplémentaires.

Si vous devez remonter d'un niveau, utilisez .. (deux points). Par exemple, imaginons que vous vous trouvez à ce niveau :

```
eShell av options>
```

saisissez .. et vous remontez d'un niveau :

```
eShell av>
```

Si vous souhaitez retourner au niveau racine depuis eShell av options> (soit deux niveaux en dessous de la racine), tapez simplement .. .. (deux points et deux points séparés par un espace). Vous remontez alors de deux niveaux, ce qui correspond dans ce cas à la racine. Vous pouvez utiliser cette méthode, quel que soit le niveau auquel vous vous trouvez dans l'arborescence. Utilisez le nombre de .. correspondant au niveau auquel vous souhaitez accéder.

Le chemin est relatif au contexte en cours. Si la commande est contenue dans le contexte en cours, n'indiquez pas de chemin. Par exemple, pour exécuter GET AV STATUS , saisissez :

GET AV STATUS - si vous êtes dans le contexte racine (la ligne de commande indique eShell>)
GET STATUS - si vous êtes dans le contexte AV (la ligne de commande indique eShell av>)
.. GET STATUS - si vous êtes dans le contexte AV OPTIONS (la ligne de commande indique eShell av options>)

Argument
Un argument est une action qui peut être réalisée pour une commande particulière. Par exemple, la commande CLEANLEVEL peut être utilisée avec les arguments suivants :

none - Ne pas nettoyer
normal - Nettoyage standard
strict - Nettoyage strict

Les arguments ENABLED ou DISABLEDpermettent d'activer ou de désactiver une fonctionnalité.

Forme abrégée/Commandes raccourcies
eShell vous permet de raccourcir les contextes, les commandes et les arguments (à condition que l'argument soit un paramètre ou une autre option). Il n'est pas possible de raccourcir un préfixe ou un argument s'il s'agit d'une valeur concrète telle qu'un nombre, un nom ou un chemin.

Voici des exemples de forme raccourcie :

```
set status disabled  => set stat en
add av exclusions C:\path\file.ext => add av exc C:\path\file.ext
```

Si deux commandes ou contextes commencent par la même lettre, ABOUT et AV, et que vous saisissez la commande raccourcie A , eShell ne parvient pas à déterminer laquelle de ces deux commandes vous souhaitez exécuter. Un message d'erreur s'affiche et répertorie les commandes commençant par un « A » pour que vous puissiez sélectionner celle à exécuter :

```
eShell>a
La commande suivante n'est pas unique : a

Les commandes suivantes sont disponibles dans ce contexte :
 ABOUT - Affiche les informations sur le programme
 AV - Passe au contexte av
```

Ensuite, l'ajout d'une ou de plusieurs lettres (AB au lieu de A) eShell exécute la commande ABOUT car cette commande est unique.

REMARQUE : afin d'avoir la garantie qu'une commande s'exécute comme vous le souhaitez, il est recommandé de ne pas abréger les commandes, les arguments, etc. et d'utiliser plutôt la forme complète. La commande s'exécute alors exactement comme vous le souhaitez et vous évite de commettre des erreurs. Ce conseil s'applique notamment pour les fichiers et les scripts de traitement par lots.

Alias
Un alias est un autre nom qui peut être utilisé pour exécuter une commande (à condition que la commande dispose d'un alias). Voici quelques alias par défaut :

(global) help - ?
(global) close - exit
(global) quit - exit
(global) bye - exit
warnlog - tools log events
virlog - tools log detections

"(global)" signifie que la commande peut être utilisée dans tous les emplacements, quel que soit le contexte actuel. Une commande peut comporter plusieurs alias. Par exemple, la commande EXIT comporte les alias CLOSE, QUIT et BYE . Si vous souhaitez quitter eShell, vous pouvez utiliser la commande EXIT proprement dite ou l'un de ses alias. L'alias VIRLOG est attribué à la commande DETECTIONS qui se trouve dans le contexte TOOLS LOG . Les détections de commande sont ainsi disponibles depuis le contexte ROOT , ce qui facilite l'accès (vous n'avez plus à saisir TOOLS puis le contexte LOG et l'exécuter directement depuis ROOT).

eShell vous permet de définir vos propres alias.

Commandes protégées
Certaines commandes sont protégées et ne peuvent être exécutées qu'après la saisie d'un mot de passe.

Guide
Lorsque vous exécutez la commande GUIDE , l'écran de première exécution apparaît et vous explique comment utiliser eShell. Cette commande est disponible dans le contexte ROOT (eShell>).

Help
Lorsque la commande HELP est utilisée seule, elle répertorie toutes les commandes disponibles, avec les préfixes et les sous-contextes du contexte actuel. Elle décrit également brièvement chaque commande/sous-contexte. Lorsque vous exécutez la commande HELP en tant qu'argument avec une commande spécifique (par exemple CLEANLEVEL HELP), vous obtenez tous les détails de cette commande. Le système affiche la SYNTAXE, les OPÉRATIONS, les ARGUMENTS et les ALIAS de la commande, ainsi qu'une brève description.

Historique de commande
eShell conserve un historique des commandes exécutées. Cet historique s'applique uniquement à la session interactive eShell en cours. Lorsque vous quittez eShell, l'historique des commandes est supprimé. Utilisez les flèches Haut et Bas de votre clavier pour parcourir l'historique. Lorsque vous avez localisé la commande que vous recherchiez, vous pouvez la réexécuter ou la modifier sans avoir à saisir l'intégralité de la commande depuis le début.

CLS/Effacement de l'écran
La commande CLS peut être utilisée pour effacer le contenu de l'écran. Cette commande fonctionne de la même manière que l'invite de commande Windows ou que toute autre interface à ligne de commande.

EXIT/CLOSE/QUIT/BYE
Pour fermer ou quitter eShell, vous pouvez utiliser l'une de ces commandes (EXIT, CLOSE, QUIT ou BYE).

4.10.2 Commandes

Cette section répertorie toutes les commandes eShell disponibles, ainsi que la description de chaque commande.

REMARQUE : Les commandes ne font pas la distinction entre les majuscules et les minuscules : que vous saisissiez les noms de commande en majuscules ou en minuscules, les commandes s'exécutent de la même manière.

Commandes contenues dans le contexte **ROOT** :

ABOUT

Répertorie les informations sur le programme. Cette commande indique le nom du produit installé, son numéro de version, les composants installés (notamment le numéro de version de chaque composant), ainsi que des informations de base sur le serveur et le système d'exploitation sur lesquels s'exécute ESET File Security.

CHEMIN DE CONTEXTE :

```
root
```

BATCH

Démarre le mode de traitement par lots d'eShell. Ce mode est très utile lors de l'exécution de fichiers/scripts en mode de traitement par lots. Il est recommandé pour les fichiers de traitement par lots. Placez `START BATCH` comme première commande dans le fichier ou le script de traitement par lots pour activer le mode de traitement par lots. Lorsque vous activez cette fonction, aucune entrée interactive (saisie d'un mot de passe par exemple) n'est demandée et les arguments manquants sont remplacés par les options par défaut. Le fichier de traitements par lots ne s'arrête pas au milieu car eShell atteint une intervention de l'utilisateur. De cette manière, le fichier de traitement par lots s'exécute sans s'arrêter (sauf en cas d'erreur ou si les commandes du fichier de traitement par lots sont incorrectes).

CHEMIN DE CONTEXTE :

```
root
```

SYNTAXE :

```
[start] batch
```

OPÉRATIONS :

`start` - Démarre le mode de traitement par lots d'eShell.

CHEMIN DE CONTEXTE :

```
root
```

EXEMPLES :

`start batch` - Démarre le mode de traitement par lots d'eShell.

GUIDE

Affiche l'écran de première exécution.

CHEMIN DE CONTEXTE :

```
root
```

PASSWORD

Normalement, lorsque vous exécutez des commandes protégées par mot de passe, vous êtes invité à taper un mot de passe pour des raisons de sécurité. Il concerne les commandes qui désactivent la protection antivirus et qui peuvent avoir une incidence sur le fonctionnement du produit ESET File Security. Vous êtes invité à saisir un mot de passe chaque fois que vous exécutez une commande de ce type. Afin d'éviter d'avoir à saisir un mot de passe à chaque fois, vous pouvez définir ce mot de passe. Il sera mémorisé par eShell et utilisé automatiquement à chaque exécution d'une commande protégée par un mot de passe. De cette manière, vous n'aurez plus à le saisir à chaque fois.

REMARQUE : le mot de passe défini ne fonctionne que pour la session interactive eShell en cours. Lorsque vous quittez eShell, ce mot de passe défini est supprimé. Lorsque vous redémarrez eShell, le mot de passe doit être redéfini.

Ce mot de passe défini est également très utile lorsque vous exécutez des fichiers/scripts de traitement par lots. Voici un exemple de fichier de traitement par lots :

```
eshell start batch "&" set password plain <votremotdepasse> "&" set status disabled
```

La commande concaténée ci-dessus démarre un mode de traitement par lots, définit le mot de passe qui sera utilisé et désactive la protection.

CHEMIN DE CONTEXTE :

```
root
```

SYNTAXE :

```
[get] | restore password
```

```
set password [plain <motdepasse>]
```

OPÉRATIONS :

get - Affiche le mot de passe

set - Définit ou efface le mot de passe

restauration - Efface le mot de passe

ARGUMENTS :

plain - Permet d'entrer le mot de passe en tant que paramètre.

password - Mot de passe.

EXEMPLES :

set password plain <votremotdepasse> - Définit un mot de passe qui sera utilisé pour les commandes protégées par mot de passe.

restore password - Efface le mot de passe.

EXEMPLES :

get password - Utilisez cette commande pour définir si le mot de passe est configuré (le mot de passe n'apparaît pas clairement ; il est remplacé par une série d'astérisques *). Si vous ne voyez aucun astérisque, cela signifie qu'aucun mot de passe n'est défini.

set password plain <votremotdepasse> - Utilisez cette commande pour configurer le mot de passe défini

restore password - Cette commande efface le mot de passe défini.

STATUS

Affiche des informations sur l'état en cours de la protection ESET File Security (identique à l'interface utilisateur graphique).

CHEMIN DE CONTEXTE :

```
root
```

SYNTAXE :

```
[get] | restore status
```

```
set status disabled | enabled
```

OPÉRATIONS :

get - Affiche l'état de la protection antivirus

set - Désactive/Active la protection antivirus

restore - Restaure les paramètres par défaut

ARGUMENTS :

disabled - Désactive la protection antivirus

`enabled` - Active la protection antivirus

EXEMPLES :

`get status` - Affiche l'état de la protection en cours

`set status disabled` - Désactive la protection

`restore status` - Restaure la protection sur le paramètre par défaut (activée)

VIRLOG

Cette commande est un alias de la commande `DETECTIONS` . Elle est utile lorsque vous devez afficher des informations sur les infiltrations détectées.

WARNLOG

Cette commande est un alias de la commande `EVENTS` . Elle est utile lorsque vous devez afficher des informations sur différents événements.

4.10.2.1 Contexte - AV

ANTISTEALTH

Active la technologie Anti-Stealth (anti-furtivité).

SYNTAXE :

`[get] | restore antistealth`

`set antistealth disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

CLEANLEVEL

Niveau de nettoyage.

SYNTAXE :

`[get] | restore cleanlevel`

`set cleanlevel none | normal | strict`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Ne pas nettoyer

`normal` - Nettoyage standard

`strict` - Nettoyage strict

EXCLUSIONS

Exclusions.

SYNTAXE :

```
[get] | clear exclusions
```

```
add | remove exclusions <exclusion>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

ARGUMENTS :

`exclusion` - Fichier/dossier/masque exclu

EXTENSIONS

Extensions analysées/exclues.

SYNTAXE :

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`extension` - Extension

`all` - Tous les fichiers

`extless` - Fichiers sans extension

SELFDEFENSE

Auto-défense.

SYNTAXE :

```
[get] | restore selfdefense
```

```
set selfdefense disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

STATUS

État de la protection antivirus.

SYNTAXE :

```
[get] | restore status
```

```
set status disabled | enabled
```

OPÉRATIONS :

`get` - Affiche l'état de la protection antivirus.

`set` - Désactive/Active la protection antivirus.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut.

ARGUMENTS :

`disabled` - Désactive la protection antivirus

`enabled` - Active la protection antivirus

4.10.2.2 Contexte - AV DOCUMENT

CLEANLEVEL

Niveau de nettoyage.

SYNTAXE :

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut.

ARGUMENTS :

`none` - Ne pas nettoyer.

`normal` - Nettoyage standard.

`strict` - Nettoyage strict.

EXTENSIONS

Extensions analysées/exclues.

SYNTAXE :

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`add` - Ajoute un élément.

`remove` - Supprime un élément.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut.

ARGUMENTS :

`extension` - Extension

`all` - Tous les fichiers

`extless` - Fichiers sans extension

INTEGRATION

Intègre la protection des documents dans le système.

SYNTAXE :

```
[get] | restore integration
```

```
set integration disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

STATUS

État en cours de la protection antivirus.

SYNTAXE :

```
[get] | restore status
```

```
set status disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.3 Contexte - AV DOCUMENT LIMITS ARCHIVE

LEVEL

Niveau d'imbrication des archives.

SYNTAXE :

```
[get] | restore level
```

```
set level <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Niveau de 1 à 20 ou 0 pour les paramètres par défaut

SIZE

Taille maximale de fichier dans l'archive (en Ko)

SYNTAXE :

```
[get] | restore size
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko (1 - 3145728) ou 0 pour les paramètres par défaut

4.10.2.4 Contexte - AV DOCUMENT LIMITS OBJECTS

SIZE

Taille de fichier maximale (Ko)

SYNTAXE :

```
[get] | restore size
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko (1 - 3145728) ou 0 pour les paramètres par défaut

TIMEOUT

Durée maximale d'analyse pour les archives (s)

SYNTAXE :

```
[get] | restore timeout
set timeout <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Durée en secondes (1 - 3600) ou 0 pour les paramètres par défaut

4.10.2.5 Contexte - AV DOCUMENT OBJECTS

ARCHIVE

Analyse les archives.

SYNTAXE :

```
[get] | restore archive
```

```
set archive disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restauration` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

BOOT

Analyse les secteurs d'amorçage.

SYNTAXE :

```
[get] | restore boot
```

```
set boot disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EMAIL

Analyse les fichiers de courriers électroniques.

SYNTAXE :

```
[get] | restore email
```

```
set email disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

FILE

Analyse les fichiers.

SYNTAXE :

```
[get] | restore file
set file disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

MEMORY

Analyse la mémoire.

SYNTAXE :

```
[get] | restore memory
set memory disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

RUNTIME

Analyse les fichiers exécutables compressés.

SYNTAXE :

```
[get] | restore runtime
set runtime disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SFX

Analyse les archives auto-extractibles.

SYNTAXE :

```
[get] | restore sfx
set sfx disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.6 Contexte - AV DOCUMENT OPTIONS

ADVHEURISTICS

Utilise l'heuristique avancée.

SYNTAXE :

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

ADWARE

Détection de logiciels espions/publicitaires/à risque

SYNTAXE :

```
[get] | restore adware
set adware disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

HEURISTICS

Utilise l'heuristique.

SYNTAXE :

```
[get] | restore heuristics
```

```
set heuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SIGNATURES

Utilise des signatures.

SYNTAXE :

```
[get] | restore signatures
set signatures disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNSAFE

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unsafe
set unsafe disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNWANTED

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unwanted
set unwanted disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.7 Contexte - AV DOCUMENT OTHER

LOGALL

Journalise tous les objets.

SYNTAXE :

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

OPTIMIZE

Optimisation intelligente.

SYNTAXE :

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.8 Contexte - AV EMAIL

ACTION

Action pour les messages infectés.

SYNTAXE :

```
[get] | restore action
```

```
set action none | delete | movedeleted | moveto
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Aucune action.

`delete` - Supprime un message.

`movedeleted` - Place dans les éléments supprimés.

`moveto` - Place dans le dossier.

CLIENTS

Clients de messagerie.

SYNTAXE :

```
[get] clients
```

```
add | remove clients <chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

ARGUMENTS :

`path` - Chemin des applications

REMARQUE : avec le filtre par application uniquement, vous devez indiquer les applications qui servent de clients de messagerie. Si une application n'est pas marquée comme client de messagerie, les messages risquent de ne pas être analysés.

QUARANTINE

Dossier des messages infectés.

SYNTAXE :

```
[get] | restore quarantine
```

```
set quarantine <chaîne>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Nom de dossier.

STATUS

État de la protection du client de messagerie.

SYNTAXE :

```
[get] | restore status
```

```
set status disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.9 Contexte - AV EMAIL GENERAL

CLEANLEVEL

Niveau de nettoyage.

SYNTAXE :

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Ne pas nettoyer

`normal` - Nettoyage standard

`strict` - Nettoyage strict

EXTENSIONS

Extensions analysées/exclues.

SYNTAXE :

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`extension` - Extension

`all` - Tous les fichiers

`extless` - Fichiers sans extension

4.10.2.10 Contexte - AV EMAIL GENERAL LIMITS ARCHIVE

NIVEAU

Niveau d'imbrication des archives.

SYNTAXE :

```
[get] | restore level
```

```
set level <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Niveau de 1 à 20 ou 0 pour les paramètres par défaut

SIZE

Taille maximale de fichier dans l'archive (en Ko)

SYNTAXE :

```
[get] | restore size
```

```
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko ou 0 pour les paramètres par défaut

4.10.2.11 Contexte - AV EMAIL GENERAL LIMITS OBJECTS

SIZE

Taille de fichier maximale (Ko).

SYNTAXE :

```
[get] | restore size
```

```
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko ou O pour les paramètres par défaut

TIMEOUT

Durée maximale d'analyse pour les archives (s).

SYNTAXE :

```
[get] | restore timeout
```

```
set timeout <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Durée en secondes ou O pour les paramètres par défaut

4.10.2.12 Contexte - AV EMAIL GENERAL OBJECTS

ARCHIVE

Analyse les archives.

SYNTAXE :

```
[get] | restore archive
```

```
set archive disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

BOOT

Analyse les secteurs d'amorçage.

SYNTAXE :

```
[get] | restore boot
```

```
set boot disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EMAIL

Analyse les fichiers de courriers électroniques.

SYNTAXE :

```
[get] | restore email
set email disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

FILE

Analyse les fichiers.

SYNTAXE :

```
[get] | restore file
set file disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

MEMORY

Analyse la mémoire.

SYNTAXE :

```
[get] | restore memory
set memory disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

RUNTIME

Analyse les fichiers exécutables compressés.

SYNTAXE :

`[get] | restore runtime`

`set runtime disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SFX

Analyse les archives auto-extractibles.

SYNTAXE :

`[get] | restore sfx`

`set sfx disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.13 Contexte - AV EMAIL GENERAL OPTIONS

ADVHEURISTICS

Utilise l'heuristique avancée.

SYNTAXE :

`[get] | restore advheuristics`

`set advheuristics disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

ADWARE

Détection de logiciels espions/publicitaires/à risque

SYNTAXE :

```
[get] | restore adware
```

```
set adware disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

HEURISTICS

Utilise l'heuristique.

SYNTAXE :

```
[get] | restore heuristics
```

```
set heuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SIGNATURES

Utilise des signatures.

SYNTAXE :

```
[get] | restore signatures
```

```
set signatures disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNSAFE

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unsafe
```

```
set unsafe disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNWANTED

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unwanted
set unwanted disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.14 Contexte - AV EMAIL GENERAL OTHER

LOGALL

Journalise tous les objets.

SYNTAXE :

```
[get] | restore logall
set logall disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

OPTIMIZE

Optimisation intelligente.

SYNTAXE :

```
[get] | restore optimize
set optimize disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.15 Contexte - AV EMAIL MESSAGE CONVERT PLAIN

Convertir le corps des messages en texte brut.

SYNTAXE :

```
[get] | restore plain
```

```
set plain disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.16 Contexte - AV EMAIL MODIFY TEMPLATE

Modèle ajouté à l'objet des messages infectés.

SYNTAXE :

```
[get] | restore template
```

```
set template [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Texte

4.10.2.17 Contexte - AV EMAIL MODIFY RECEIVED

BODY

Ajouter une notification aux messages reçus et lus.

SYNTAXE :

```
[get] | restore body
```

```
set body never | infected | all
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`never` - Ne pas ajouter.

`infected` - Courriers infectés uniquement.

`all` - Tous les messages

SUBJECT

Ajouter une notification à l'objet des messages infectés reçus et lus.

SYNTAXE :

```
[get] | restore subject
```

```
set subject disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.18 Contexte - AV EMAIL MODIFY SENT

BODY

Ajouter une notification aux messages reçus et lus.

SYNTAXE :

```
[get] | restore body
```

```
set body never | infected | all
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`never` - Ne pas ajouter.

`infected` - Courriers infectés uniquement.

`all` - Tous les messages

SUBJECT

Ajouter une notification à l'objet des messages infectés reçus et lus.

SYNTAXE :

```
[get] | restore subject
```

```
set subject disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.19 Contexte - AV EMAIL OEXPRESS/WINMAIL

INTEGRATION

S'intègre à Outlook Express et Windows Mail.

SYNTAXE :

```
[get] | restore integration
```

```
set integration disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.20 Contexte - AV EMAIL OUTLOOK

FORCEADDIN

Utiliser le complément COM dans les anciennes versions de Microsoft Outlook.

SYNTAXE :

```
[get] | restore forceaddin
```

```
set forceaddin 2010newer | 2007newer | allversions
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`2010newer` - Microsoft Outlook 2010 et versions supérieures

`2007newer` - Microsoft Outlook 2007 et versions supérieures

`allversions` - Toutes les versions Microsoft Outlook

INTEGRATION

S'intègre à Microsoft Outlook.

SYNTAXE :

```
[get] | restore integration
```

```
set integration disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SYNCFIX

Active la résolution des conflits de synchronisation dans Microsoft Outlook.

SYNTAXE :

```
[get] | restore syncfix
```

```
set syncfix <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

`0` - Désactivé `3` - Entièrement activé, autres valeurs possibles.

4.10.2.21 Contexte - AV EMAIL OUTLOOK RESCAN

ONCHANGE

Désactive la vérification au changement de contenu de la boîte aux lettres.

SYNTAXE :

```
[get] | restore onchange
```

```
set onchange disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.22 Contexte - AV EMAIL PROTOCOL POP3

COMPATIBILITY

Configuration de la compatibilité.

SYNTAXE :

```
[get] | restore compatibility
```

```
set compatibility compatible | both | effective
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`compatible` - Niveau de compatibilité maximal

`both` - Niveau de compatibilité moyen

`effective` - Efficacité maximale.

REMARQUE : les clients de messagerie ne fonctionnent pas tous correctement avec le filtrage POP3 en mode standard. Les paramètres suivants permettent d'ajuster le niveau de compatibilité pour résoudre les conflits potentiels. Toutefois, l'augmentation du niveau de compatibilité peut réduire l'efficacité de la surveillance Internet ou empêcher de bénéficier de l'intégralité de ses fonctionnalités.

PORTS

Ports utilisés par le protocole POP3.

SYNTAXE :

```
[get] | restore ports
```

```
set ports [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Numéros de port délimités par une virgule.

USE

Contrôle le protocole POP3.

SYNTAXE :

```
[get] | restore use
```

```
set use disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.23 Contexte - AV EMAIL PROTOCOL POP3S

COMPATIBILITY

Configuration de la compatibilité.

SYNTAXE :

```
[get] | restore compatibility
```

```
set compatibility compatible | both | effective
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`compatible` - Niveau de compatibilité maximal

`both` - Niveau de compatibilité moyen

`effective` - Efficacité maximale.

REMARQUE : les clients de messagerie ne fonctionnent pas tous correctement avec le filtrage POP3S en mode standard. Les paramètres suivants permettent d'ajuster le niveau de compatibilité pour résoudre les conflits potentiels. Toutefois, l'augmentation du niveau de compatibilité peut réduire l'efficacité de la surveillance Internet ou empêcher de bénéficier de l'intégralité de ses fonctionnalités.

MODE

Mode de filtrage POP3S.

SYNTAXE :

```
[get] | restore mode
```

```
set mode none | ports | clients
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Ne pas utiliser le contrôle du protocole POP3.

`ports` - Utilise le contrôle de protocole POP3S pour les ports sélectionnés.

`clients` - Utilise le contrôle de protocole POP3S pour les applications marquées comme clients de messagerie qui utilisent les ports sélectionnés.

PORTS

Ports utilisés par le protocole POP3S.

SYNTAXE :

```
[get] | restore ports
```

```
set ports [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Numéros de port délimités par une virgule.

4.10.2.24 Contexte - AV EMAIL RESCAN

ONUPDATE

Répéter l'analyse après mise à jour.

SYNTAXE :

```
[get] | restore onupdate
```

```
set onupdate disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.25 Contexte - AV EMAIL SCAN

OTHERMODULES

Accepte les résultats d'analyse d'autres modules.

SYNTAXE :

```
[get] | restore othermodules
```

```
set othermodules disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

PLAIN

Analyse le corps des messages en texte brut.

SYNTAXE :

```
[get] | restore plain
set plain disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

READ

Analyse les messages lus.

SYNTAXE :

```
[get] | restore read
set read disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

RECEIVED

Analyse les messages reçus.

SYNTAXE :

```
[get] | restore received
set received disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

RTF

Analyse le corps des messages en RTF.

SYNTAXE :

```
[get] | restore rtf
set rtf disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SENT

Analyse les messages envoyés.

SYNTAXE :

```
[get] | restore sent
set sent disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.26 Contexte - AV EMAIL THUNDERBIRD

INTEGRATION

S'intègre à Mozilla Thunderbird.

SYNTAXE :

```
[get] | restore integration
set integration disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.27 Contexte - AV EMAIL WINLIVE

INTEGRATION

S'intègre à Windows Live Mail.

SYNTAXE :

```
[get] | restore integration
```

```
set integration disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.28 Contexte - AV LIMITS ARCHIVE

NIVEAU

Niveau d'imbrication des archives.

SYNTAXE :

```
[get] | restore level
```

```
set level <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Niveau de 1 à 20 ou 0 pour les paramètres par défaut

TAILLE

Taille maximale de fichier dans l'archive (en Ko)

SYNTAXE :

```
[get] | restore size
```

```
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko ou 0 pour les paramètres par défaut

4.10.2.29 Contexte - AV LIMITS OBJECTS

TAILLE

Taille de fichier maximale (Ko).

SYNTAXE :

```
[get] | restore size
```

```
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko ou O pour les paramètres par défaut

TIMEOUT

Durée maximale d'analyse pour les archives (s).

SYNTAXE :

```
[get] | restore timeout
```

```
set timeout <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Durée en secondes ou O pour les paramètres par défaut

4.10.2.30 Contexte - AV NETFILTER

AUTOSTART

Exécute automatiquement le filtrage de contenu des protocoles d'application HTTP et POP3.

SYNTAXE :

```
[get] | restore autostart
```

```
set autostart disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EXCLUDED

Applications exclues du filtrage de protocole.

SYNTAXE :

```
[get] excluded
```

```
add | remove excluded <chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

ARGUMENTS :

`path` - Chemin des applications

MODE

Redirige le trafic pour le filtrage.

SYNTAXE :

```
[get] | restore mode
```

```
set mode ports | application | both
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`ports` - Ports HTTP et POP3.

`application` - Applications marquées comme navigateurs Internet ou clients de messagerie.

`both` - Ports et applications marqués comme navigateurs Internet ou clients de messagerie.

STATUS

Active le filtrage de contenu des protocoles d'application HTTP et POP3.

SYNTAXE :

```
[get] | restore status
```

```
set status disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.31 Contexte - AV NETFILTER PROTOCOL SSL

BLOCKSSL2

Bloque les communications chiffrées à l'aide du protocole obsolète SSL v2.

SYNTAXE :

```
[get] | restore blockssl2
set blockssl2 disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EXCEPTIONS

Applique les exceptions créées sur la base de certificats.

SYNTAXE :

```
[get] | restore exceptions
set exceptions disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

MODE

Mode de filtrage SSL.

SYNTAXE :

```
[get] | restore mode
set mode allways | ask | none
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`always` - Toujours analyser le contrôle du protocole SSL.

`ask` - Interroger sur les sites non visités (possibilité de définir des exclusions).

`none` - Ne pas utiliser le contrôle du protocole SSL.

4.10.2.32 Contexte - AV NETFILTER PROTOCOL SSL CERTIFICATE

ADDTOBROWSERS

Ajoute le certificat racine aux navigateurs connus.

SYNTAXE :

```
[get] | restore addtobrowsers
```

```
set addtobrowsers disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

REMARQUE : Pour vérifier correctement le trafic crypté en SSL, le certificat racine pour ESET, spol. s r.o utilisé pour signer de certificats sera ajouté à la base de certificat Trusted Root Certification Authorities (TRCA).

EXCLUDED

Liste des certificats exclus du filtrage de contenu.

SYNTAXE :

```
[get] excluded
```

```
 remove excluded <nom>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`remove` - Supprime un élément

ARGUMENTS :

`name` - Nom du certificat

NOTTRUSTED

Non fiable si le certificat est non valide ou endommagé.

SYNTAXE :

```
[get] | restore nottrusted
```

```
set nottrusted ask | block
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`ask` - Interroge sur la validité du certificat.

`block` - Bloque toute communication utilisant le certificat.

TRUSTED

Liste des certificats approuvés.

SYNTAXE :

```
[get] trusted
remove trusted <nom>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`remove` - Supprime un élément

ARGUMENTS :

`name` - Nom du certificat

UNKNOWNROOT

Racine inconnue s'il est impossible de vérifier le certificat à l'aide du TRCA.

SYNTAXE :

```
[get] | restore unknownroot
set unknownroot ask | block
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`ask` - Interroge sur la validité du certificat.

`block` - Bloque toute communication utilisant le certificat.

4.10.2.33 Contexte - AV OBJECTS

ARCHIVE

Analyse les archives.

SYNTAXE :

```
[get] | restore archive
set archive disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

BOOT

Analyse les secteurs d'amorçage.

SYNTAXE :

```
[get] | restore boot
```

`set boot disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EMAIL

Analyse les fichiers de courriers électroniques.

SYNTAXE :

`[get] | restore email`

`set email disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

MEMORY

Analyse la mémoire.

SYNTAXE :

`[get] | restore memory`

`set memory disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

RUNTIME

Analyse les fichiers exécutables compressés.

SYNTAXE :

`[get] | restore runtime`

`set runtime disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SFX

Analyse les archives auto-extractibles.

SYNTAXE :

```
[get] | restore sfx
```

```
set sfx disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.34 Contexte - AV OPTIONS

ADVHEURISTICS

Utilise l'heuristique avancée.

SYNTAXE :

```
[get] | restore advheuristics
```

```
set advheuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

HEURISTICS

Utilise l'heuristique.

SYNTAXE :

```
[get] | restore heuristics
```

```
set heuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNSAFE

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unsafe
set unsafe disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNWANTED

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unwanted
set unwanted disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.35 Contexte - AV OTHER

LOGALL

Journalise tous les objets.

SYNTAXE :

```
[get] | restore logall
set logall disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

OPTIMIZE

Optimisation intelligente.

SYNTAXE :

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.36 Contexte - AV REALTIME

AUTOSTART

Démarre automatiquement la protection en temps réel.

SYNTAXE :

```
[get] | restore autostart
```

```
set autostart disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

CLEANLEVEL

Niveau de nettoyage.

SYNTAXE :

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Ne pas nettoyer

`normal` - Nettoyage standard

`strict` - Nettoyage strict

EXTENSIONS

Extensions analysées/exclues.

SYNTAXE :

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`extension` - Extension

`all` - Tous les fichiers

`extless` - Fichiers sans extension

STATUS

État de la protection en temps réel de l'ordinateur.

SYNTAXE :

```
[get] | restore status
```

```
set status disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.37 Contexte - AV REALTIME DISK

FLOPPY

Analyse le support amovible.

SYNTAXE :

```
[get] | restore floppy
```

```
set floppy disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

LOCAL

Analyse les disques locaux.

SYNTAXE :

```
[get] | restore local
set local disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

NETWORK

Analyse les lecteurs réseau.

SYNTAXE :

```
[get] | restore network
set network disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.38 Contexte - AV REALTIME EVENT

CREATE

Analyse les fichiers lors de la création.

SYNTAXE :

```
[get] | restore create
set create disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EXECUTE

Analyse les fichiers lors de l'exécution.

SYNTAXE :

```
[get] | restore execute
```

```
set execute disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

FLOPPYACCESS

Analyse lors de l'accès à la disquette.

SYNTAXE :

```
[get] | restore floppyaccess
```

```
set floppyaccess disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

OPEN

Analyse les fichiers à l'ouverture.

SYNTAXE :

```
[get] | restore open
```

```
set open disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SHUTDOWN

Analyse lors de l'arrêt de l'ordinateur.

SYNTAXE :

```
[get] | restore shutdown
set shutdown disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.39 Contexte - AV REALTIME EXECUTABLE

ADVHEURISTICS

Active l'heuristique avancée à l'exécution du fichier.

SYNTAXE :

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.40 Contexte - AV REALTIME EXECUTABLE FROMREMOVABLE

ADVHEURISTICS

Active l'heuristique avancée lors de l'exécution du fichier depuis le support amovible.

SYNTAXE :

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EXCLUSION

Exclusions de lecteur USB.

SYNTAXE :

```
[get] | restore exclusion
```

```
select exclusion none | <lecteur> | all
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`select` - Sélectionne un élément.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Désélectionne tous les disques.

`drive` - Lettre d'un disque à sélectionner/désélectionner.

`all` - Sélectionne tous les disques.

REMARQUE : utilisez cette option pour autoriser les exceptions de l'analyse à l'aide de l'heuristique avancée lors de l'exécution du fichier. Les paramètres d'heuristique avancée pour les disques durs seront appliqués aux périphériques sélectionnés.

4.10.2.41 Contexte - AV REALTIME LIMITS ARCHIVE

NIVEAU

Niveau d'imbrication des archives.

SYNTAXE :

```
[get] | restore level
```

```
set level <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Niveau de 1 à 20 ou 0 pour les paramètres par défaut

TAILLE

Taille maximale de fichier dans l'archive (en Ko)

SYNTAXE :

```
[get] | restore size
```

```
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko ou O pour les paramètres par défaut

4.10.2.42 Contexte - AV REALTIME LIMITS OBJECTS

TAILLE

Taille de fichier maximale (Ko).

SYNTAXE :

```
[get] | restore size
```

```
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko ou O pour les paramètres par défaut

TIMEOUT

Durée maximale d'analyse pour les archives (s).

SYNTAXE :

```
[get] | restore timeout
```

```
set timeout <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Durée en secondes ou O pour les paramètres par défaut

4.10.2.43 Contexte - AV REALTIME OBJECTS

ARCHIVE

Analyse les archives.

SYNTAXE :

```
[get] | restore archive
```

```
set archive disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

BOOT

Analyse les secteurs d'amorçage.

SYNTAXE :

```
[get] | restore boot
```

```
set boot disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EMAIL

Analyse les fichiers de courriers électroniques.

SYNTAXE :

```
[get] | restore email
```

```
set email disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

MEMORY

Analyse la mémoire.

SYNTAXE :

```
[get] | restore memory
```

```
set memory disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

RUNTIME

Analyse les fichiers exécutables compressés.

SYNTAXE :

```
[get] | restore runtime
```

```
set runtime disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SFX

Analyse les archives auto-extractibles.

SYNTAXE :

```
[get] | restore sfx
```

```
set sfx disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.44 Contexte - AV REALTIME ONWRITE

ADVHEURISTICS

Active l'heuristique avancée pour les nouveaux fichiers et les fichiers modifiés.

SYNTAXE :

```
[get] | restore advheuristics
```

```
set advheuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

RUNTIME

Analyse les nouvelles archives exécutables et les archives exécutables modifiées.

SYNTAXE :

```
[get] | restore runtime
set runtime disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SFX

Analyse les nouvelles archives auto-extractibles et les archives auto-extractibles modifiées.

SYNTAXE :

```
[get] | restore sfx
set sfx disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.45 Contexte - AV REALTIME ONWRITE ARCHIVE

LEVEL

Niveau d'imbrication des archives.

SYNTAXE :

```
[get] | restore level
set level <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Niveau (0 - 20)

TAILLE

Taille maximum d'un fichier d'archive analysé (Ko).

SYNTAXE :

```
[get] | restore size
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille (Ko).

4.10.2.46 Contexte - AV REALTIME OPTIONS

ADVHEURISTICS

Utilise l'heuristique avancée.

SYNTAXE :

```
[get] | restore advheuristics
set advheuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

HEURISTICS

Utilise l'heuristique.

SYNTAXE :

```
[get] | restore heuristics
set heuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNSAFE

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unsafe
set unsafe disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNWANTED

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unwanted
```

```
set unwanted disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.47 Contexte - AV REALTIME OTHER

LOGALL

Journalise tous les objets.

SYNTAXE :

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

OPTIMIZE

Optimisation intelligente.

SYNTAXE :

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.48 Contexte - AV REALTIME REMOVABLE

BLOCK

Bloque les supports amovibles.

SYNTAXE :

```
[get] | restore block
```

```
set block disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EXCLUSION

Supports amovibles autorisés.

SYNTAXE :

```
[get] | restore exclusion
```

```
select exclusion none | <lecteur> | all
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`select` - Sélectionne un élément.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Désélectionne tous les disques.

`drive` - Lettre d'un disque à sélectionner/désélectionner.

`all` - Sélectionne tous les disques.

REMARQUE : utilisez cette option pour autoriser l'accès au support amovible (CD, disquettes, clés USB). Le marquage d'un support supprime les restrictions d'accès lors de la tentative d'accès à ce support.

4.10.2.49 Contexte - AV WEB

BROWSERS

Navigateurs Internet.

SYNTAXE :

```
[get] browsers
```

```
add | remove browsers <chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

ARGUMENTS :

`path` - Chemin des applications

REMARQUE : pour augmenter la sécurité, il est conseillé de marquer toute application utilisée comme navigateur Internet, en activant la case appropriée. Le transfert de données des applications non marquées comme navigateur Web risque de ne pas être analysé.

CLEANLEVEL

Niveau de nettoyage.

SYNTAXE :

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Ne pas nettoyer

`normal` - Nettoyage standard

`strict` - Nettoyage strict

EXTENSIONS

Extensions analysées/exclues.

SYNTAXE :

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`extension` - Extension

`all` - Tous les fichiers

`extless` - Fichiers sans extension

STATUS

Protection de l'accès Web.

SYNTAXE :

```
[get] | restore status
```

```
set status disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.50 Contexte - AV WEB ADDRESSMGMT

ADDRESS

Gestion des adresses dans la liste sélectionnée.

SYNTAXE :

```
[get] | clear address
```

```
add | remove address <adresse>
```

```
import | export address <chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`import` - Importe du fichier.

`export` - Exporte dans le fichier.

`clear` - Supprime tous les éléments/fichiers.

ARGUMENTS :

`address` - Adresse

`path` - Chemin du fichier.

LISTE

Gestion de la liste d'adresses.

SYNTAXE :

```
[get] | restore list
```

```
set list <nomliste> disabled | enabled
```

`select | remove list <nomliste>`

`add list allowed <nomliste> | blocked <nomliste> | excluded <nomliste>`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`select` - Sélectionner pour la modification.

`add` - Ajoute un élément

`remove` - Supprime un élément

ARGUMENTS :

`listname` - Nom de la liste.

`disabled` - Ne pas utiliser la liste.

`enabled` - Utiliser la liste.

`allowed` - Liste des adresses autorisées.

`blocked` - Liste des adresses bloquées.

`excluded` - Liste des adresses exclues du filtrage.

REMARQUE : Pour modifier la liste sélectionnée (marquée d'un - x), utilisez la commande « `av web addressmgmt address` ».

NOTIFY

Notifier lors de l'application d'une adresse de la liste.

SYNTAXE :

`[get] | restore notify`

`set notify disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

WHITELISTED

N'autoriser l'accès qu'aux adresses HTTP figurant dans la liste des adresses autorisées.

SYNTAXE :

`[get] | restore whitelisted`

`set whitelisted disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.51 Contexte - AV WEB LIMITS ARCHIVE

LEVEL

Niveau d'imbrication des archives.

SYNTAXE :

```
[get] | restore level
```

```
set level <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Niveau de 1 à 20 ou 0 pour les paramètres par défaut

TAILLE

Taille maximale de fichier dans l'archive (en Ko)

SYNTAXE :

```
[get] | restore size
```

```
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko ou 0 pour les paramètres par défaut

4.10.2.52 Contexte - AV WEB LIMITS OBJECTS

TAILLE

Taille de fichier maximale (Ko).

SYNTAXE :

```
[get] | restore size
```

```
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko ou 0 pour les paramètres par défaut

TIMEOUT

Durée maximale d'analyse pour les archives (s).

SYNTAXE :

```
[get] | restore timeout
set timeout <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Durée en secondes ou O pour les paramètres par défaut

4.10.2.53 Contexte - AV WEB OBJECTS

ARCHIVE

Analyse les archives.

SYNTAXE :

```
[get] | restore archive
set archive disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

BOOT

Analyse les secteurs d'amorçage.

SYNTAXE :

```
[get] | restore boot
set boot disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EMAIL

Analyse les fichiers de courriers électroniques.

SYNTAXE :

`[get] | restore email`

`set email disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

FILE

Analyse les fichiers.

SYNTAXE :

`[get] | restore file`

`set file disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

MEMORY

Analyse la mémoire.

SYNTAXE :

`[get] | restore memory`

`set memory disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

RUNTIME

Analyse les fichiers exécutables compressés.

SYNTAXE :

`[get] | restore runtime`

`set runtime disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SFX

Analyse les archives auto-extractibles.

SYNTAXE :

`[get] | restore sfx`

`set sfx disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.54 Contexte - AV WEB OPTIONS

ADVHEURISTICS

Utilise l'heuristique avancée.

SYNTAXE :

`[get] | restore advheuristics`

`set advheuristics disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

ADWARE

Détection de logiciels espions/publicitaires/à risque

SYNTAXE :

`[get] | restore adware`

`set adware disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

HEURISTICS

Utilise l'heuristique.

SYNTAXE :

```
[get] | restore heuristics
```

```
set heuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SIGNATURES

Utilise des signatures.

SYNTAXE :

```
[get] | restore signatures
```

```
set signatures disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNSAFE

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unsafe
```

```
set unsafe disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNWANTED

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unwanted

set unwanted disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.55 Contexte - AV WEB OPTIONS BROWSERS

ACTIVEMODE

Mode actif pour les navigateurs Web.

SYNTAXE :

```
[get] activemode

add | remove activemode <chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

ARGUMENTS :

`path` - Chemin des applications

REMARQUE : les programmes ajoutés à la liste sont ajoutés automatiquement à la liste des navigateurs Internet.

4.10.2.56 Contexte - AV WEB OTHER

LOGALL

Journalise tous les objets.

SYNTAXE :

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

OPTIMIZE

Optimisation intelligente.

SYNTAXE :

```
[get] | restore optimize
```

```
set optimize disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.57 Contexte - AV WEB PROTOCOL HTTP

PORTS

Ports utilisés par le protocole HTTP.

SYNTAXE :

```
[get] | restore ports
```

```
set ports [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Numéros de port séparés par un signe deux-points.

USE

Analyse HTTP.

SYNTAXE :

```
[get] | restore use
```

```
set use disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.58 Contexte - AV WEB PROTOCOL HTTPS

MODE

Mode de filtrage HTTPS.

SYNTAXE :

```
[get] | restore mode
```

```
set mode none | ports | browsers
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Ne pas utiliser le contrôle du protocole.

`ports` - Utiliser le contrôle de protocole HTTPS pour les ports sélectionnés.

`browsers` - Utiliser le contrôle de protocole HTTPS pour les applications marquées comme navigateurs qui utilisent les ports sélectionnés.

PORTS

Ports utilisés par le protocole HTTPS.

SYNTAXE :

```
[get] | restore ports
```

```
set ports [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Numéros de port délimités par une virgule.

4.10.2.59 Contexte - GENERAL

CONFIG

Importer/exporter les paramètres.

SYNTAXE :

```
import | export config <chemin>
```

OPÉRATIONS :

`import` - Importe du fichier.

`export` - Exporte dans le fichier.

ARGUMENTS :

`path` - Chemin du fichier.

LICENSE

Gestion de licences.

SYNTAXE :

```
[get] license
```

```
import license <chemin>
```

```
export license <ID> <chemin>
```

```
remove license <ID>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`remove` - Supprime un élément

`import` - Importe du fichier.

`export` - Exporte dans le fichier.

ARGUMENTS :

`path` - Chemin du fichier de licence.

`ID` - ID de tâche.

4.10.2.60 Contexte - GENERAL ACCESS

ADMIN

Protection des paramètres des droits d'administrateur.

SYNTAXE :

```
[get] | restore admin
```

```
set admin disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

BATCH

Exécuter les commandes entrées en tant qu'arguments lors de l'exécution d'eShell.

SYNTAXE :

```
[get] | restore batch
```

```
set batch disabled | <heure> | allways
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactivé

`time` - Intervalle en minutes (1 - 1440 minutes)

`toujours` - Toujours

PASSWORD

Ce mot de passe est utilisé pour les commandes protégées par mot de passe. Normalement, lorsque vous exécutez des commandes protégées par mot de passe, vous êtes invité à taper un mot de passe. Ce mot de passe est paramétré pour des raisons de sécurité. Il s'applique aux commandes qui désactivent la protection antivirus et qui peuvent avoir une incidence sur le fonctionnement du produit ESET File Security. Vous êtes invité à saisir un mot de passe chaque fois que vous exécutez une commande de ce type. Vous avez également la possibilité de définir ce mot de passe pour votre session eShell en cours ; dans ce cas, vous ne serez plus invité à le saisir. Pour plus d'informations, cliquez ici.

Si vous utilisez la saisie interactive du mot de passe (recommandé), ne complétez pas les paramètres. Pour réinitialiser le mot de passe, ne remplissez pas la zone du mot de passe.

CHEMIN DE CONTEXTE :

```
general access
```

SYNTAXE :

```
[get] | restore | set password
```

OPÉRATIONS :

`get` - Affiche le mot de passe

`set` - Définit le mot de passe.

`restore` - Redéfinit le mot de passe.

EXEMPLES :

`get password` - Utilisez cette commande pour définir si le mot de passe est configuré (le mot de passe n'apparaît pas clairement ; il est remplacé par une série d'astérisques *). Si vous ne voyez aucun astérisque, cela signifie qu'aucun mot de passe n'est défini.

`set password` - Utilisez cette commande pour définir le mot de passe ; entrez-le simplement (si aucun mot de passe n'est entré, la protection des paramètres n'est pas utilisée).

`restore password` - Cette commande efface le mot de passe existant (la protection des paramètres n'est pas utilisée).

ÉQUIVALENT DANS L'INTERFACE UTILISATEUR GRAPHIQUE :

cliquez ici pour afficher la configuration à l'aide de l'interface utilisateur graphique.

4.10.2.61 Contexte - GENERAL ESHELL

ALIAS

Gestion d'alias.

SYNTAXE :

```
[get] | clear | restore alias
```

```
add alias [.] <alias>=<commande>
```

```
remove alias <alias>
```

```
import | export alias <chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`import` - Importe du fichier.

`export` - Exporte dans le fichier.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`.` - Crée un alias global.

`alias` - Nouvel alias.

`command` - Commande associée (la validité de la commande n'est pas vérifiée).

`alias` - Alias à supprimer.

`path` - Chemin du fichier.

LISTER

Utiliser la liste.

SYNTAXE :

```
[get] | restore lister
```

```
set lister disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.62 Contexte - GENERAL ESHELL COLOR

ALIAS

Couleur d'alias.

SYNTAXE :

`[get] | restore alias`

`set alias [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

COMMAND

Couleur des commandes.

SYNTAXE :

`[get] | restore command`

`set command [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

CONTEXT

Couleur du contexte.

SYNTAXE :

```
[get] | restore context

set context [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

DEFAULT

Couleur de base.

SYNTAXE :

```
[get] | restore default
```

```
set default [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

DISABLED

Couleur S/O.

SYNTAXE :

```
[get] | restore disabled
```

```
set disabled [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan |
red | magenta | yellow | white]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

ERROR

Couleur des messages d'erreur.

SYNTAXE :

```
[get] | restore error
```

```
set error [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red |
magenta | yellow | white]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

INTERACTIVE

Couleur des opérations interactives.

SYNTAXE :

```
[get] | restore interactive
```

```
set interactive [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan |
red | magenta | yellow | white]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

LIST1

Couleur de liste 1.

SYNTAXE :

```
[get] | restore list1
```

```
set list1 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

LIST2

Couleur de liste 2.

SYNTAXE :

```
[get] | restore list2
```

```
set list2 [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red | magenta | yellow | white]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

SUCCESS

Couleur de l'état correct.

SYNTAXE :

```
[get] | restore success

set success [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

WARNING

Couleur des messages d'avertissement.

SYNTAXE :

```
[get] | restore warning
```

```
set warning [black | navy | grass | ltblue | brown | purple | olive | ltgray | gray | blue | green | cyan | red
| magenta | yellow | white]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`black` - Noir

`navy` - Bleu marine

`grass` - Vert gazon

`ltblue` - Bleu clair

`brown` - Marron

`purple` - Violet

`olive` - Vert olive

`ltgray` - Gris clair

`gray` - Gris

`blue` - Bleu

`green` - Vert

`cyan` - Cyan

`red` - Rouge

`magenta` - Magenta

`yellow` - Jaune

`white` - Blanc

4.10.2.63 Contexte - GENERAL ESHELL OUTPUT

UTF8

Sortie codée UTF8.

SYNTAXE :

```
[get] | restore utf8
```

```
set utf8 disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

REMARQUE : pour un affichage correct, la ligne de commande doit utiliser une police TrueType de type Lucida Console.

4.10.2.64 Contexte - GENERAL ESHELL STARTUP

LOADCOMMANDS

Charge toutes les commandes au démarrage.

SYNTAXE :

```
[get] | restore loadcommands
```

```
set loadcommands disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

STATUS

Affiche l'état de protection au démarrage.

SYNTAXE :

```
[get] | restore status
```

```
set status disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.65 Contexte - GENERAL ESHELL VIEW

CMDHELP

Afficher l'aide en cas de défaillance d'une commande.

SYNTAXE :

```
[get] | restore cmdhelp
```

```
set cmdhelp disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

COLORS

Utilise des couleurs.

SYNTAXE :

```
[get] | restore colors
set colors disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

FITWIDTH

Couper le texte pour qu'il corresponde à la largeur.

SYNTAXE :

```
[get] | restore fitwidth
set fitwidth disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

GLOBAL

Affiche les commandes globales.

SYNTAXE :

```
[get] | restore global
set global disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

HIDDEN

Affiche les commandes masquées.

SYNTAXE :

```
[get] | restore hidden
```

```
set hidden disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

OPERATIONS

Affiche les opérations dans la liste des commandes.

SYNTAXE :

```
[get] | restore operations
```

```
set operations disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SHORTLIST

Affiche une présélection de commandes concernant le changement de contexte.

SYNTAXE :

```
[get] | restore shortlist
```

```
set shortlist disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SYNTAXHINT

Affiche les conseils sur la syntaxe des commandes.

SYNTAXE :

```
[get] | restore syntaxhint
```

```
set syntaxhint disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

VALUESONLY

Affiche uniquement des valeurs sans description.

SYNTAXE :

```
[get] | restore valuesonly
```

```
set valuesonly disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.66 Contexte - GENERAL PERFORMANCE

SCANNERS

Nombre d'analyses en cours.

SYNTAXE :

```
[get] | restore scanners
```

```
set scanners <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Nombre (1 - 20)

4.10.2.67 Contexte - GENERAL PROXY

ADDRESS

Adresse du serveur proxy.

SYNTAXE :

```
[get] | restore address
```

```
set address [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Adresse

DETECT

Détecte la configuration du serveur proxy.

SYNTAXE :

```
detect
```

LOGIN

Nom de connexion.

SYNTAXE :

```
[get] | restore login
```

```
set login [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Nom

PASSWORD

Mot de passe du serveur proxy.

SYNTAXE :

```
[get] | restore password
```

```
set password [plain <motdepasse>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre.

`mot de passe` - Mot de passe

PORT

Port

SYNTAXE :

```
[get] | restore port
```

```
set port <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Numéro de port

USE

Utilise un serveur proxy.

SYNTAXE :

```
[get] | restore use
```

```
set use disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.68 Contexte - GENERAL QUARANTINE RESCAN

UPDATE

Analyse les fichiers en quarantaine après chaque mise à jour.

SYNTAXE :

```
[get] | restore update
```

```
set update disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

restore - Restaure les paramètres/l'objet/le fichier par défaut.

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.69 Contexte - GENERAL REMOTE

INTERVAL

Intervalle de connexion (minutes).

SYNTAXE :

```
[get] | restore interval
```

```
set interval <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Durée en minutes (1 - 1 440)

USE

Connexion à ESET Remote Administrator Server.

SYNTAXE :

```
[get] | restore use
```

```
set use disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.70 Contexte - GENERAL REMOTE SERVER PRIMARY

ADDRESS

Adresse d'ESET Remote Administrator Server.

SYNTAXE :

```
[get] | restore address
```

```
set address [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Adresse

ENCRYPT

Bloque la connexion non codée.

SYNTAXE :

```
[get] | restore encrypt
```

```
set encrypt disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

PASSWORD

Mot de passe d'ESET Remote Administrator Server.

SYNTAXE :

```
[get] | restore password
```

```
set password [plain <motdepasse>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre.

`mot de passe` - Mot de passe

PORT

Port d'ESET Remote Administrator Server.

SYNTAXE :

```
[get] | restore port
```

```
set port <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Numéro de port

4.10.2.71 Contexte - GENERAL REMOTE SERVER SECONDARY

ADDRESS

Adresse d'ESET Remote Administrator Server.

SYNTAXE :

```
[get] | restore address
```

```
set address [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Adresse

ENCRYPT

Bloque la connexion non codée.

SYNTAXE :

```
[get] | restore encrypt
```

```
set encrypt disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

PASSWORD

Mot de passe d'ESET Remote Administrator Server.

SYNTAXE :

```
[get] | restore password
```

```
set password [plain <motdepasse>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre.

`password` - Mot de passe

PORT

Port d'ESET Remote Administrator Server.

SYNTAXE :

```
[get] | restore port
set port <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Numéro de port

4.10.2.72 Contexte - GENERAL TS.NET

EXCLUSION

Exclure de la soumission.

SYNTAXE :

```
[get] | restore exclusion
add | remove exclusion <exclusion>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`exclusion` - Extension

FROM

Adresse électronique du contact

SYNTAXE :

```
[get] | restore from
set from [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Adresse électronique

LOGING

Création de journal.

SYNTAXE :

[get] | restore loging

set loging disabled | enabled

OPÉRATIONS :

get - Renvoie le paramètre/l'état en cours.

set - Définit la valeur/l'état.

restore - Restaure les paramètres/l'objet/le fichier par défaut.

ARGUMENTS :

disabled - Désactive la fonction/le paramètre.

enabled - Active la fonction/le paramètre.

SENDING

Soumission de fichiers suspects.

SYNTAXE :

```
[get] | restore sending
```

```
set sending none | ask | auto
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Ne pas envoyer.

`ask` - Confirmer avant l'envoi pour analyse.

`auto` - Envoi pour analyse sans confirmation.

VIA

Mode d'envoi du fichier.

SYNTAXE :

```
[get] | restore via
```

```
set via auto | ra | direct
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`auto` - Via ESET Remote Administrator ou directement à ESET

`ra` - Via ESET Remote Administrator

`direct` - Directement à ESET

WHEN

Quand soumettre les fichiers suspects.

SYNTAXE :

```
[get] | restore when
```

```
set when asap | update
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`asap` - Dès que possible.

`update` - Pendant la mise à jour.

4.10.2.73 Contexte - GENERAL TS.NET STATISTICS

SENDING

Soumission d'informations statistiques.

SYNTAXE :

```
[get] | restore sending
set sending disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

WHEN

Soumission d'informations statistiques anonymes.

SYNTAXE :

```
[get] | restore when
set when asap | update
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`asap` - Dès que possible.

`update` - Pendant la mise à jour.

4.10.2.74 Contexte - SCANNER

CLEANLEVEL

Niveau de nettoyage.

SYNTAXE :

```
[get] | restore cleanlevel
```

```
set cleanlevel none | normal | strict
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Ne pas nettoyer

`normal` - Nettoyage standard

`strict` - Nettoyage strict

EXTENSIONS

Extensions analysées/exclues.

SYNTAXE :

```
[get] | restore extensions
```

```
add | remove extensions <extension> | /all | /extless
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`extension` - Extension

`all` - Tous les fichiers

`extless` - Fichiers sans extension

PROFILE

Gestion du profil d'analyse de l'ordinateur.

SYNTAXE :

```
[get] profile
```

```
select | remove profile <nom>
```

```
add profile new: <nom> [copyfrom: <nom>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`select` - Sélectionne un élément.

`add` - Ajoute un élément

`remove` - Supprime un élément

ARGUMENTS :

`name` - Nom du profil.

`new` - Nouveau profil.

`copyfrom` - Copier les paramètres depuis le profil.

REMARQUE : pour accéder aux autres commandes de contexte, reportez-vous au profil actif (marqué d'un - x). Pour sélectionner le profil actif, sélectionnez `select scanner profile <nom du profil>`.

SCAN

Analyse d'ordinateur.

SYNTAXE :

```
[get] | clear scan
```

```
start scan [readonly]
```

```
pause | resume | stop scan <ID> | all
```

OPÉRATIONS :

`get` - Affiche les analyses en cours et terminées.

`start` - Effectue une analyse d'ordinateur pour le profil sélectionné.

`stop` - Arrêter l'analyse.

`resume` - Continue l'analyse interrompue.

`pause` - Interrompt l'analyse.

`clear` - Supprime les analyses terminées de la liste.

ARGUMENTS :

`readonly` - Analyse sans nettoyage.

`ID` - ID de l'analyse pour l'exécution de la commande.

`all` - Exécute la commande pour toutes les analyses.

TARGET

Cibles d'analyse pour le profil actif.

SYNTAXE :

```
[get] target
```

```
add | remove target <chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

ARGUMENTS :

`path` - Chemin/Cible d'analyse.

REMARQUE : pour l'analyse du secteur d'amorçage, saisissez `X:\${Boot}` 'xétant le nom du disque analysé.

4.10.2.75 Contexte - SCANNER LIMITS ARCHIVE

LEVEL

Niveau d'imbrication des archives.

SYNTAXE :

```
[get] | restore level
set level <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Niveau de 1 à 20 ou 0 pour les paramètres par défaut

TAILLE

Taille maximale de fichier dans l'archive (en Ko)

SYNTAXE :

```
[get] | restore size
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko ou 0 pour les paramètres par défaut

4.10.2.76 Contexte - SCANNER LIMITS OBJECTS

TAILLE

Taille de fichier maximale (Ko).

SYNTAXE :

```
[get] | restore size
set size <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille en Ko ou 0 pour les paramètres par défaut

TIMEOUT

Durée maximale d'analyse pour les archives (s).

SYNTAXE :

```
[get] | restore timeout
```

```
set timeout <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Durée en secondes ou 0 pour les paramètres par défaut

4.10.2.77 Contexte - SCANNER OBJECTS

ARCHIVE

Analyse les archives.

SYNTAXE :

```
[get] | restore archive
```

```
set archive disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

BOOT

Analyse les secteurs d'amorçage.

SYNTAXE :

```
[get] | restore boot
```

```
set boot disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

EMAIL

Analyse les fichiers de courriers électroniques.

SYNTAXE :

```
[get] | restore email
```

```
set email disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

MEMORY

Analyse la mémoire.

SYNTAXE :

```
[get] | restore memory
```

```
set memory disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

RUNTIME

Analyse les fichiers exécutables compressés.

SYNTAXE :

```
[get] | restore runtime
```

```
set runtime disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SFX

Analyse les archives auto-extractibles.

SYNTAXE :

```
[get] | restore sfx
```

```
set sfx disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.78 Contexte - SCANNER OPTIONS

ADVHEURISTICS

Utilise l'heuristique avancée.

SYNTAXE :

```
[get] | restore advheuristics
```

```
set advheuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

HEURISTICS

Utilise l'heuristique.

SYNTAXE :

```
[get] | restore heuristics
```

```
set heuristics disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNSAFE

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unsafe
```

```
set unsafe disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

UNWANTED

Détection d'applications potentiellement indésirables.

SYNTAXE :

```
[get] | restore unwanted
```

```
set unwanted disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.79 Contexte - SCANNER OTHER

ADS

Analyser les flux de données alternatifs (ADS).

SYNTAXE :

```
[get] | restore ads
```

```
set ads disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

LOGALL

Journalise tous les objets.

SYNTAXE :

```
[get] | restore logall
```

```
set logall disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

LOWPRIORITY

Exécuter les analyses en arrière-plan avec une priorité faible.

SYNTAXE :

`[get] | restore lowpriority`

`set lowpriority disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

OPTIMIZE

Optimisation intelligente.

SYNTAXE :

`[get] | restore optimize`

`set optimize disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

PRESERVETIME

Conserve la date et l'heure du dernier accès.

SYNTAXE :

`[get] | restore preservetime`

`set preservetime disabled | enabled`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

SCROLL

Fait défiler le journal de l'analyse.

SYNTAXE :

```
[get] | restore scroll
set scroll disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.80 Contexte - SERVER

AUTOEXCLUSIONS

Gestion des exclusions automatiques.

SYNTAXE :

```
[get] | restore autoexclusions
select autoexclusions <serveur>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`select` - Sélectionne un élément.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`server` - Nom de serveur.

4.10.2.81 Contexte - TOOLS

QUARANTINE

Quarantaine.

SYNTAXE :

```
[get] quarantine
add quarantine <chemin>
send | remove | restore quarantine <ID>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

`send` - Envoie un élément/fichier.

ARGUMENTS :

`path` - Chemin du fichier.

`ID` - ID de fichier en quarantaine

STATISTICS

Statistiques.

SYNTAXE :

```
[get] | clear statistics
```

OPÉRATIONS :

`get` - Affiche les statistiques.

`clear` - Réinitialise les statistiques.

SYSINSPECTOR

SysInspector.

SYNTAXE :

```
[get] sysinspector

add | remove sysinspector <nom>

export sysinspector <nom> to:<chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`export` - Exporte dans le fichier.

ARGUMENTS :

`name` - Commentaire.

`path` - Nom de fichier (.zip ou .xml).

4.10.2.82 Contexte - TOOLS ACTIVITY

FILESYSTEM

Activité du système de fichiers.

SYNTAXE :

```
[get] filesystem [<nombre>] [seconds | minutes | hours [<année>-<mois>]]
```

ARGUMENTS :

`count` - Nombre d'entrées à afficher.

`seconds` - Échantillonnage d'1 seconde.

`minutes` - Échantillonnage d'1 minute.

`heures` - Échantillonnage d'1 heure.

`year` - Année à afficher

`month` - Mois à afficher

4.10.2.83 Contexte - TOOLS LOG

DETECTIONS

Ce procédé est utile lorsque vous devez afficher des informations sur les infiltrations détectées.

CHEMIN DE CONTEXTE :

```
root
```

SYNTAXE :

```
[get] detections [count <nombre>] [from <année>-<mois>-<jour> <heure>:<minute>:<seconde>] [to <année>-<mois>-<jour> <h
```

```
clear detections
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`clear` - Supprime tous les éléments/fichiers.

ARGUMENTS :

`count` - Affiche le nombre d'entrées sélectionnées.

`number` - Nombre d'entrées.

`from` - Affiche les entrées de l'heure indiquée.

`year` - Année.

`month` - Mois.

`jour` - Jour.

`hour` - Heure.

`minute` - Minute.

`second` - Seconde.

`to` - Affiche les entrées jusqu'à l'heure sélectionnée.

ALIAS :

```
virlog
```

EXEMPLES :

`get detections from 2011-04-14 01:30:00` - Affiche toutes les infiltrations détectées après le 14 avril 2011 01:30:00 (lors de la définition de la date, vous devez inclure l'heure et la commande pour que l'instruction fonctionne correctement).

`clear detections` - Efface l'intégralité du journal.

EVENTS

Cette commande est utile lorsque vous devez afficher des informations sur différents événements.

SYNTAXE :

```
[get] events [count <nombre>] [from <année>-<mois>-<jour> <heure>:<minute>:<seconde>] [to <année>-<mois>-<jour>
<heure>:<minute>:<seconde>]
```

```
clear events
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`clear` - Supprime tous les éléments/fichiers.

ARGUMENTS :

`count` - Affiche le nombre d'entrées sélectionnées.

`number` - Nombre d'entrées.

`from` - Affiche les entrées de l'heure indiquée.

`year` - Année.

`month` - Mois.

`jour` - Jour.

`hour` - Heure.

`minute` - Minute.

`seconde` - Seconde.

`to` - Affiche les entrées jusqu'à l'heure sélectionnée.

ALIAS :

```
warnlog
```

EXEMPLES :

`get events from 2011-04-14 01:30:00` - Affiche tous les événements qui se sont produits après le 14 avril 2011 01:30:00 (lors de la définition de la date, vous devez inclure l'heure et la commande pour que l'instruction fonctionne correctement).

`clear events` - Efface l'intégralité du journal.

FILTER

Verbosité minimale des événements à afficher.

SYNTAXE :

```
[get] | restore filter
```

```
set filter [[none] [critical] [errors] [warnings] [informative] [diagnostic] [all]] [smart]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Aucune entrée.

`critical` - Erreurs critiques.

`errors` - Erreurs.

`warnings` - Avertissements.

`informative` - Entrées informatives.

`diagnostic` - Entrées de diagnostic.

`all` - Toutes les entrées.

`smart` - Filtrage intelligent.

SCANS

Journal d'analyse d'ordinateur ou liste des journaux.

SYNTAXE :

```
[get] scans [id <id>] [count <nombre>] [from <année>-<mois>-<jour> <heure>:<minute>:<seconde>] [to <année>-
```

`<mois>-<jour> <heure>:<minute>:<seconde>]`

`effacer les analyses`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`clear` - Supprime tous les éléments/fichiers.

ARGUMENTS :

`id` - Affiche les détails de l'analyse d'ordinateur avec l'ID.

`id` - ID d'analyse.

`count` - Affiche uniquement le nombre d'entrées sélectionnées.

`number` - Nombre d'entrées.

`from` - Affiche uniquement les entrées à partir de l'heure sélectionnée.

`year` - Année.

`month` - Mois.

`jour` - Jour.

`hour` - Heure.

`minute` - Minute.

`second` - Seconde.

`to` - Affiche uniquement les entrées à partir de l'heure sélectionnée.

VERBOSITY

Verbosité minimale des journaux.

SYNTAXE :

`[get] | restore verbosity`

`set verbosity critical | errors | warnings | informative | diagnostic`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`critical` - Erreurs critiques.

`errors` - Erreurs.

`warnings` - Avertissements.

`informative` - Entrées informatives.

`diagnostic` - Entrées de diagnostic.

4.10.2.84 Contexte - TOOLS LOG CLEANING

TIMEOUT

Durée de vie des entrées du journal (jours).

SYNTAXE :

```
[get] | restore timeout
set timeout <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Jour (1 - 365).

USE

Suppression automatique du journal.

SYNTAXE :

```
[get] | restore use
set use disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.85 Contexte - TOOLS LOG OPTIMIZE

LEVEL

Optimisation par dépassement du nombre d'entrées inutilisées (pourcentage).

SYNTAXE :

```
[get] | restore level
set level <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Pourcentage d'entrées inutilisées (1 - 100).

NOW

Optimise immédiatement les fichiers de protocole.

SYNTAXE :

```
now
```

L'exécution de la command peut prendre quelques minutes.

USE

Optimisation automatique du journal.

SYNTAXE :

```
[get] | restore use
```

```
set use disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.86 Contexte - TOOLS NOTIFICATION

VERBOSITY

Verbosité minimale des notifications.

SYNTAXE :

```
[get] | restore verbosity
```

```
set verbosity critical | errors | warnings | informative | diagnostic
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`critical` - Erreurs critiques.

`errors` - Erreurs.

`warnings` - Avertissements.

`informative` - Entrées informatives.

`diagnostic` - Entrées de diagnostic.

4.10.2.87 Contexte - TOOLS NOTIFICATION EMAIL

FROM

Adresse électronique des expéditeurs.

SYNTAXE :

```
[get] | restore from
```

```
set from [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Adresse électronique

LOGIN

Nom de connexion.

SYNTAXE :

```
[get] | restore login
```

```
set login [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Nom

PASSWORD

Mot de passe.

SYNTAXE :

```
[get] | restore password
```

```
set password [plain <motdepasse>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre.

`password` - Mot de passe

SERVER

Adresse du serveur SMTP.

SYNTAXE :

```
[get] | restore server
```

```
set server [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Adresse

TO

Adresse électronique des destinataires.

SYNTAXE :

```
[get] | restore to
```

```
set to [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Adresse électronique

USE

Envoi d'événements par e-mail.

SYNTAXE :

```
[get] | restore use
```

```
set use disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.88 Contexte - TOOLS NOTIFICATION MESSAGE

ENCODING

Codage des messages d'avertissement.

SYNTAXE :

```
[get] | restore encoding
```

```
set encoding nolocal | localcharset | localencoding | ISO-2022-JP
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`nolocal` - Ne pas utiliser les caractères de l'alphabet en vigueur.

`localcharset` - Utiliser les caractères de l'alphabet en vigueur.

`localencoding` - Utiliser les caractères de l'alphabet en vigueur et le codage.

`ISO` - Utiliser le codage ISO-2022-JP (pour la version japonaise uniquement).

4.10.2.89 Contexte - TOOLS NOTIFICATION MESSAGE FORMAT

DETECTION

Format des messages d'avertissement de menace.

SYNTAXE :

```
[get] | restore detection
```

```
set detection [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Format des messages.

Options du format des messages.

`%TimeStamp%` - Date et heure de l'événement

`%Scanner%` - Module qui a détecté l'événement.

`%ComputerName%` - Nom de l'ordinateur.

`%ProgramName%` - Programme qui a provoqué l'événement.

`%ErrorDescription%` - Description d'erreur.

En ce qui concerne le format du message, vous devez remplacer les mots-clés (répertoriés ici entre des signes de pourcentage « % ») par les valeurs correspondantes.

REMARQUE : les messages et avertissements concernant les virus ESET File Security ont le format par défaut. Il n'est pas recommandé de changer ce format. Vous pouvez en revanche le modifier si vous utilisez le système de gestion automatique des messages.

EVENT

Format d'événement.

SYNTAXE :

```
[get] | restore event
```

```
set event [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Format des messages.

Options du format des messages.

`%TimeStamp%` - Date et heure de l'événement

`%Scanner%` - Module qui a détecté l'événement.

`%ComputerName%` - Nom de l'ordinateur.

`%ProgramName%` - Programme qui a provoqué l'événement.

`%InfectedObject%` - Objet infecté (fichier, message).

`%VirusName%` - Nom de virus.

En ce qui concerne le format du message, vous devez remplacer les mots-clés (répertoriés ici entre des signes de pourcentage « % ») par les valeurs correspondantes.

REMARQUE : les messages et avertissements concernant les virus ESET File Security ont le format par défaut. Il n'est pas recommandé de changer ce format. Vous pouvez en revanche le modifier si vous utilisez le système de gestion automatique des messages.

4.10.2.90 Contexte - TOOLS NOTIFICATION WINPOPUP

ADDRESS

Envoie des notifications aux noms des ordinateurs.

SYNTAXE :

```
[get] | restore address
```

```
set address [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Nom d'ordinateur séparé par une virgule.

TIMEOUT

Intervalle d'envoi aux ordinateurs du réseau local.

SYNTAXE :

```
[get] | restore timeout
```

```
set timeout <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Intervalle en secondes (1 - 3 600)

USE

Envoi d'événements aux ordinateurs du réseau local.

SYNTAXE :

```
[get] | restore use
```

```
set use disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.91 Contexte - TOOLS SCHEDULER

ACTION

Tâche planifiée.

SYNTAXE :

```
[get] action
```

```
set action external | logmaintenance | startupcheck | status | scan | update
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`external` - Exécute une application externe.

`logmaintenance` - Maintenance des journaux.

`startupcheck` - Analyse au démarrage.

`status` - Crée un instantané du statut de l'ordinateur.

`scan` - Analyse d'ordinateur.

`update` - Mise à jour.

TASK

Tâches planifiées.

SYNTAXE :

```
[get] | select task [<ID>]

set task <ID> disabled | enabled

add task <nom_tâche>

remove | start task <ID>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

`select` - Sélectionne un élément.

`add` - Ajoute un élément

`remove` - Supprime un élément

`start` - Démarre la tâche.

ARGUMENTS :

`ID` - ID de tâche.

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

`task_name` - Nom de la tâche.

TRIGGER

Exécution de tâche.

SYNTAXE :

```
[get] trigger

set trigger once | repeat | daily | weekly | event
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`once` - Une fois.

`repeat` - Plusieurs fois.

`daily` - Quotidiennement.

`weekly` - Chaque semaine.

`event` - Déclenchée par un événement.

4.10.2.92 Contexte - TOOLS SCHEDULER EVENT

INTERVAL

Exécute la tâche une seule fois dans l'intervalle spécifié (heures).

SYNTAXE :

```
[get] interval

set interval <heures>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`hours` - Durée en heures (1 - 720 heures)

TYPE

Tâche déclenchée par un événement.

SYNTAXE :

```
[get] type
```

```
set type startup | startuponcedaily | dialup | engineupdate | appupdate | logon | detection
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`startup` - Au démarrage de l'ordinateur.

`startuponcedaily` - Au premier démarrage de l'ordinateur chaque jour.

`dialup` - Connexion commutée à Internet/VPN.

`engineupdate` - Mise à jour de la base des signatures de virus.

`appupdate` - Mise à jour des composants du programme.

`logon` - Ouverture de session de l'utilisateur.

`detection` - Détection de menace.

4.10.2.93 Contexte - TOOLS SCHEDULER FAILSAFE

EXECUTE

Action à entreprendre si la tâche n'est pas exécutée.

SYNTAXE :

```
[get] execute
```

```
set execute asap | iftimeout | no
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`asap` - Exécute la tâche dès que possible.

`iftimeout` - Exécute la tâche immédiatement si l'intervalle spécifié depuis sa dernière exécution est dépassé.

`no` - Ne pas exécuter avec retard.

REMARQUE : pour définir une limite, saisissez `SET TOOLS SCHEDULER EDIT FAILSAFE TIMEOUT <HEURES>`.

TIMEOUT

Intervalle de la tâche (heures).

SYNTAXE :

```
[get] timeout
```

```
set timeout <heures>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`hours` - Durée en heures (1 - 720 heures)

4.10.2.94 Contexte - TOOLS SCHEDULER PARAMETERS CHECK

LEVEL

Niveau d'analyse.

SYNTAXE :

```
[get] level
set level [before_logon | after_logon | most_frequent | frequent | common | rare | all]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`before_logon` - Fichiers exécutés avant la connexion de l'utilisateur.

`after_logon` - Fichiers exécutés après la connexion de l'utilisateur.

`most_frequent` - Seulement les fichiers les plus fréquemment utilisés.

`frequent` - Fichiers fréquemment utilisés.

`common` - Fichiers couramment utilisés.

`rare` - Fichiers rarement utilisés.

`all` - Fichiers enregistrés.

PRIORITY

Priorité de l'analyse.

SYNTAXE :

```
[get] priority
set priority [normal | low | lowest | idle]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`normal` - Normale.

`low` - Inférieure.

`lowest` - Minimale.

`idle` - Quand inactif.

4.10.2.95 Contexte - TOOLS SCHEDULER PARAMETERS EXTERNAL

ARGUMENTS

Arguments.

SYNTAXE :

```
[get] arguments
```

```
set arguments <arguments>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`arguments` - Arguments

DIRECTORY

Dossier de travail.

SYNTAXE :

```
[get] directory
```

```
set directory <chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`path` - Chemin.

EXECUTABLE

Fichier exécutable.

SYNTAXE :

```
[get] executable
```

```
set executable <chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`path` - Chemin.

4.10.2.96 Contexte - TOOLS SCHEDULER PARAMETERS SCAN

PROFILE

Profil d'analyse.

SYNTAXE :

```
[get] profile
```

```
set profile <profil>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`profile` - Nom du profil.

READONLY

Analyse sans nettoyage.

SYNTAXE :

```
[get] readonly
```

```
set readonly disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`set` - Définit la valeur/l'état

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

TARGET

Cibles à analyser.

SYNTAXE :

```
[get] | clear target
```

```
add | remove target <chemin>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours

`add` - Ajoute un élément

`remove` - Supprime un élément

`clear` - Supprime tous les éléments/fichiers.

ARGUMENTS :

`path` - Chemin/Cible d'analyse.

4.10.2.97 Contexte - TOOLS SCHEDULER PARAMETERS UPDATE

PRIMARY

Profil de mise à jour.

SYNTAXE :

```
[get] primary
```

```
set primary [<profil>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

ARGUMENTS :

`profile` - Nom du profil.

SECONDARY

Autre profil de mise à jour.

SYNTAXE :

```
[get] secondary
```

```
set secondary [<profil>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

ARGUMENTS :

`profile` - Nom du profil.

4.10.2.98 Contexte - TOOLS SCHEDULER REPEAT

INTERVAL

Intervalle de la tâche (minutes).

SYNTAXE :

```
[get] interval
```

```
set interval <minutes>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

ARGUMENTS :

`minutes` - Durée en heures (1 - 720 heures).

4.10.2.99 Contexte - TOOLS SCHEDULER STARTUP

DATE

La tâche sera exécutée à la date sélectionnée.

SYNTAXE :

```
[get] date
set date <année>-<mois>-<jour>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

ARGUMENTS :

`year` - Année.

`month` - Mois.

`jour` - Jour.

DAYS

Exécuter la tâche les jours suivants.

SYNTAXE :

```
[get] days
set | add | remove days none | [monday] [tuesday] [wednesday] [thurdsday] [friday] [saturday] [sunday] | all
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`add` - Ajoute un élément

`remove` - Supprime un élément

ARGUMENTS :

`none` - Aucun jour indiqué.

`monday` - Lundi.

`tuesday` - Mardi.

`wednesday` - Mercredi.

`thursday` - Jeudi.

`friday` - Vendredi.

`saturday` - Samedi.

`sunday` - Dimanche.

`all` - Chaque jour.

TIME

La tâche sera exécutée à l'heure sélectionnée.

SYNTAXE :

```
[get] time
set time <heure>:<minute>:<seconde>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

ARGUMENTS :

`hour` - Heure.

`minute` - Minute.

`seconde` - Seconde.

4.10.2.100 Contexte - UPDATE

CACHE

Vide le cache de mise à jour.

SYNTAXE :

```
clear cache
```

COMPONENTS

Met à jour les composants du programme.

SYNTAXE :

```
[get] | restore components
```

```
set components never | allways | ask
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`never` - Ne pas mettre à jour.

`always` - Toujours mettre à jour.

`ask` - Demander avant de télécharger les composants du programme.

LOGIN

Nom de connexion.

SYNTAXE :

```
[get] | restore login
```

```
set login [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Nom

REMARQUE : Entrez ici le nom d'utilisateur et le mot de passe reçus après l'achat ou l'activation. Il est vivement recommandé de copier (Ctrl+C) ces informations figurant dans le message d'enregistrement et de les coller (Ctrl+V).

PASSWORD

Mot de passe.

SYNTAXE :

```
[get] | restore password
```

```
set password [plain <motdepasse>]
```

OPÉRATIONS :

`get` - Affiche le mot de passe

`set` - Définit ou supprime le mot de passe.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre

`password` - Mot de passe

REMARQUE : Entrez ici le nom d'utilisateur et le mot de passe reçus après l'achat ou l'activation. Il est vivement recommandé de copier (Ctrl+C) ces informations figurant dans le message d'enregistrement et de les coller (Ctrl+V).

PRERELEASE

Active les mises à jour des versions bêta.

SYNTAXE :

```
[get] | restore prerelease
```

```
set prerelease disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

PROFILE

Met à jour la gestion des profils.

SYNTAXE :

```
[get] profile
```

```
select | remove profile <nom>
```

```
add profile new: <nom> [copyfrom: <nom>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`select` - Sélectionne un élément.

`add` - Ajoute un élément

`remove` - Supprime un élément

ARGUMENTS :

`name` - Nom du profil.

`new` - Nouveau profil.

`copyfrom` - Copie les paramètres depuis le profil.

REMARQUE : pour accéder aux autres commandes de contexte, reportez-vous au profil actif (marqué d'un - x). Pour sélectionner le profil actif, sélectionnez `select update profile <nom du profil>`.

SERVER

Serveurs de mise à jour.

SYNTAXE :

```
[get] | restore server
```

```
select | add | remove server <serveur>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`select` - Sélectionne un élément.

`add` - Ajoute un élément

`remove` - Supprime un élément

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`server` - Adresse du serveur.

STATUS

Affiche l'état de la mise à jour.

SYNTAXE :

```
[get] status
```

UPDATE

Mise à jour.

SYNTAXE :

```
start | stop update
```

OPÉRATIONS :

`start` - Exécute la mise à jour.

`stop` - Annule la mise à jour.

4.10.2.101 Contexte - UPDATE CONNECTION

DISCONNECT

Se déconnecte du serveur après la mise à jour.

SYNTAXE :

```
[get] | restore disconnect
```

```
set disconnect disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

LOGIN

Nom d'utilisateur.

SYNTAXE :

```
[get] | restore login
set login [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Nom

PASSWORD

Mot de passe.

SYNTAXE :

```
[get] | restore password
set password [plain <motdepasse>]
```

OPÉRATIONS :

`get` - Affiche le mot de passe

`set` - Définit ou supprime le mot de passe.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre

`password` - Mot de passe

RUNAS

Se connecte au réseau local comme.

SYNTAXE :

```
[get] | restore runas
set runas system | current | specified
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`system` - Compte système (par défaut).

`current` - Utilisateur actuel.

`specified` - Utilisateur spécifié.

4.10.2.102 Contexte - UPDATE MIRROR

COMPONENTS

Met à jour les composants du programme.

SYNTAXE :

```
[get] | start | restore components
```

```
set components disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`start` - Démarre la mise à jour.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

DOSSIER

Dossier de stockage des fichiers en miroir.

SYNTAXE :

```
[get] | restore folder
```

```
set folder [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Chemin des dossiers.

LOGIN

Nom d'utilisateur.

SYNTAXE :

```
[get] | restore login
```

```
set login [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Nom

PASSWORD

Mot de passe.

SYNTAXE :

```
[get] | restore password
set password [plain <motdepasse>]
```

OPÉRATIONS :

`get` - Affiche le mot de passe

`set` - Définit ou supprime le mot de passe.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre

`password` - Mot de passe

USE

Crée un miroir de mise à jour.

SYNTAXE :

```
[get] | restore use
set use disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

VERSIONS

Met à jour la gestion des versions.

SYNTAXE :

```
[get] | restore versions
select versions <version>
```

OPÉRATIONS :

`get` - Affiche les versions disponibles.

`select` - Sélectionne/Désélectionne la version mise à jour.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`version` - Nom de version.

4.10.2.103 Contexte - UPDATE MIRROR CONNECTION

DISCONNECT

Se déconnecte du serveur après la mise à jour.

SYNTAXE :

```
[get] | restore disconnect
```

```
set disconnect disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

LOGIN

Nom d'utilisateur.

SYNTAXE :

```
[get] | restore login
```

```
set login [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Nom

PASSWORD

Mot de passe.

SYNTAXE :

```
[get] | restore password
```

```
set password [plain <motdepasse>]
```

OPÉRATIONS :

`get` - Affiche le mot de passe

`set` - Définit ou supprime le mot de passe.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre

`password` - Mot de passe

RUNAS

Se connecte au réseau local comme.

SYNTAXE :

```
[get] | restore runas
set runas system | current | specified
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`system` - Compte système (par défaut).

`current` - Utilisateur actuel.

`specified` - Utilisateur spécifié.

4.10.2.104 Contexte - UPDATE MIRROR SERVER

AUTHENTICATION

Utilise l'authentification.

SYNTAXE :

```
[get] | restore authentication
set authentication none | basic | ntlm
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`none` - Non.

`basic` - De base.

`ntlm` - NTLM

PORT

Port.

SYNTAXE :

```
[get] | restore port
set port <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Numéro de port

USE

Fournit les fichiers de mise à jour via un serveur HTTP interne.

SYNTAXE :

```
[get] | restore use
```

```
set use disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

4.10.2.105 Contexte - UPDATE NOTIFICATION

DOWNLOAD

Demander avant de télécharger une mise à jour.

SYNTAXE :

```
[get] | restore download
```

```
set download disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

HIDE

Ne pas afficher de notification de réussite de la mise à jour.

SYNTAXE :

```
[get] | restore hide
```

```
set hide disabled | enabled
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`disabled` - Désactive la fonction/le paramètre

`enabled` - Active la fonction/le paramètre

TAILLE

Demander si un fichier de mise à jour a une taille supérieure à (Ko).

SYNTAXE :

`[get] | restore size`

`set size <nombre>`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Taille du fichier (Ko).

REMARQUE : pour désactiver les notifications de mise à jour, saisissez `0`.

4.10.2.106 Contexte - UPDATE PROXY

LOGIN

Nom d'utilisateur.

SYNTAXE :

`[get] | restore login`

`set login [<chaîne>]`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Nom

MODE

Configuration du proxy HTTP.

SYNTAXE :

`[get] | restore mode`

`set mode global | noproxy | userdefined`

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`global` - Utiliser les paramètres globaux de serveur proxy.

`noproxy` - Ne pas utiliser de serveur proxy.

`userdefined` - Connexion via un serveur proxy.

PASSWORD

Mot de passe.

SYNTAXE :

`[get] | restore password`

`set password [plain <motdepasse>]`

OPÉRATIONS :

`get` - Affiche le mot de passe

`set` - Définit ou supprime le mot de passe.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`plain` - Permet d'entrer le mot de passe en tant que paramètre

`password` - Mot de passe

PORT

Port du serveur proxy.

SYNTAXE :

```
[get] | restore port
```

```
set port <nombre>
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`number` - Numéro de port

SERVER

Serveur proxy.

SYNTAXE :

```
[get] | restore server
```

```
set server [<chaîne>]
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`string` - Adresse du serveur.

4.10.2.107 Contexte - UPDATE SYSTEM

NOTIFY

Avertir l'utilisateur concernant les mises à jour manquantes à partir du niveau.

SYNTAXE :

```
[get] | restore notify
```

```
set notify no | optional | recommended | important | critical
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`non` - Non.

`optional` - Facultatif.

`recommended` - Recommandé.

`important` - Important.

`critical` - Critique.

RESTART

Redémarrer l'ordinateur après une mise à jour des composants du programme.

SYNTAXE :

```
[get] | restore restart
```

```
set restart never | ask | auto
```

OPÉRATIONS :

`get` - Renvoie le paramètre/l'état en cours.

`set` - Définit la valeur/l'état.

`restore` - Restaure les paramètres/l'objet/le fichier par défaut

ARGUMENTS :

`never` - Ne pas redémarrer.

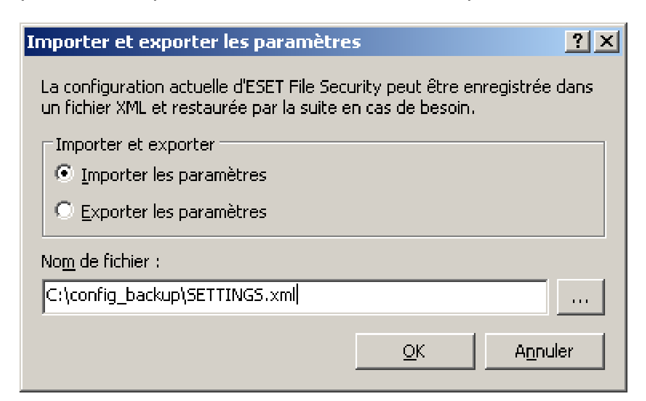
`ask` - Demander avant de redémarrer.

`auto` - Redémarrer automatiquement.

4.11 Importer et exporter les paramètres

Les configurations d'importation et d'exportation de ESET File Security sont accessibles dans **Configuration** en cliquant sur **Importer** et **exporter les paramètres**.

L'importation et l'exportation utilisent le type de fichier .xml. Ces opérations sont utiles si vous devez sauvegarder la configuration actuelle d'ESET File Security pour l'utiliser ultérieurement. L'option Exporter les paramètres est également pratique pour les utilisateurs qui souhaitent utiliser leur configuration ESET File Security préférée sur plusieurs systèmes. Il leur suffit d'importer un fichier .xml pour transférer les paramètres souhaités.



4.12 ThreatSense.Net

Le système d'alerte anticipé ThreatSense.Net est un outil qui permet d'informer ESET immédiatement et en permanence de l'existence de nouvelles infiltrations. Le système d'alerte anticipé bidirectionnel ThreatSense.Net n'a qu'un seul objectif : améliorer la protection que nous vous offrons. Le meilleur moyen d'être sûr de détecter les nouvelles menaces dès qu'elles apparaissent est de rester en contact permanent avec le plus grand nombre de nos clients et de les utiliser comme des éclaireurs. Deux options sont possibles :

1. Vous pouvez décider de ne pas activer le système d'alerte anticipé ThreatSense.Net. Vous ne perdez rien de la fonctionnalité du logiciel et vous bénéficiez toujours la meilleure protection que nous offrons.

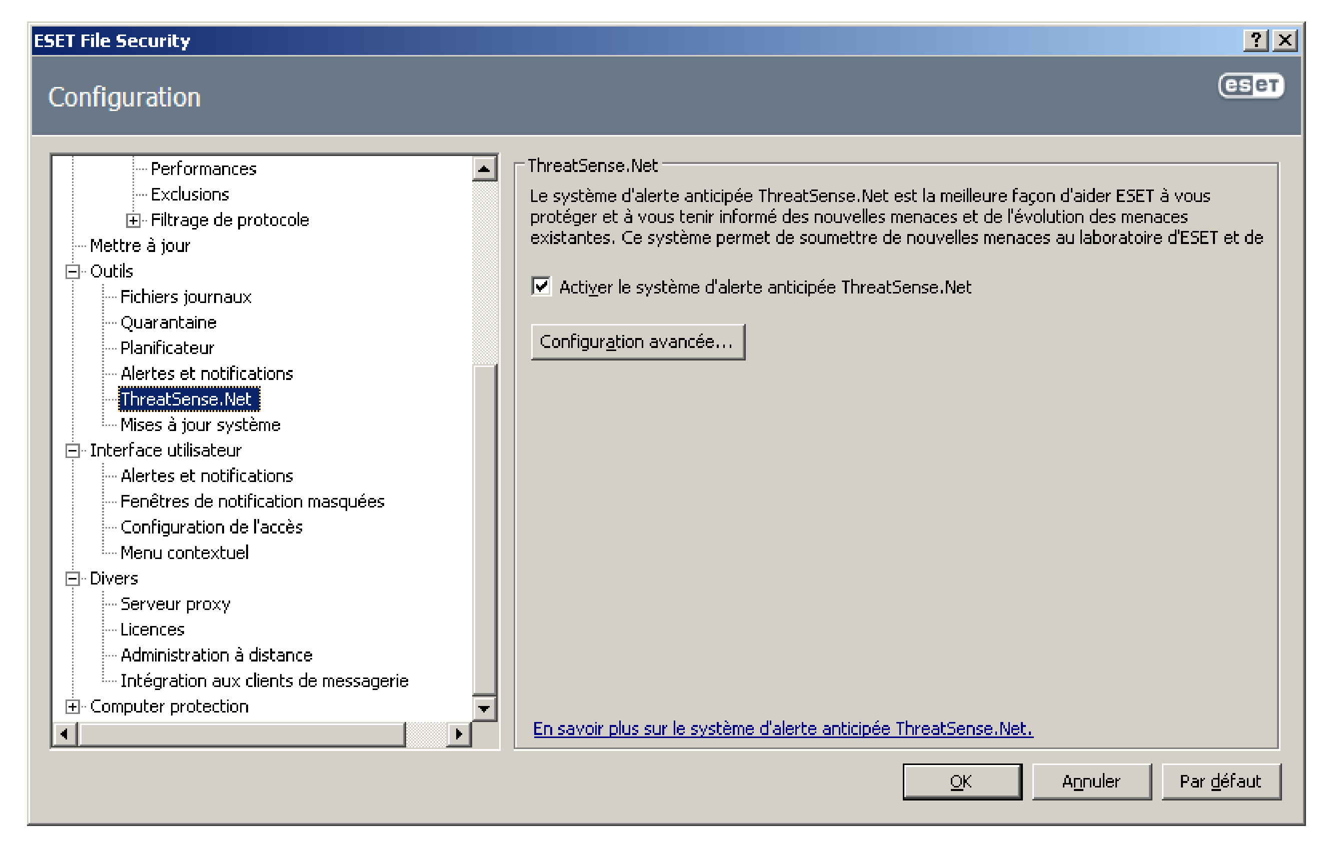
2. Vous pouvez configurer le système d'alerte anticipé ThreatSense.Net afin d'envoyer des informations anonymes qui concernent les nouvelles menaces et indiquent l'endroit où se trouve le code menaçant. Ce fichier peut être envoyé à ESET pour une analyse détaillée. En étudiant ces menaces, ESET améliore ses capacités à détecter les menaces.

Le système d'alerte anticipé ThreatSense.Net collecte sur votre ordinateur des informations concernant les nouvelles menaces détectées. Ces informations comprennent un échantillon ou une copie du fichier dans lequel la menace est apparue, le chemin et le nom du fichier, la date et l'heure, le processus par lequel la menace est apparue sur votre ordinateur et des informations sur le système d'exploitation de votre ordinateur.

Certaines informations vous concernant ou concernant votre ordinateur (noms d'utilisateur dans un chemin de répertoire) sont divulguées au laboratoire de recherche sur les menaces d'ESET, mais ces informations ne sont utilisées à AUCUNE autre fin que pour répondre immédiatement aux nouvelles menaces.

Par défaut, ESET File Security est configuré pour demander confirmation avant de soumettre au laboratoire d'ESET les fichiers suspects pour une analyse détaillée. Les fichiers ayant une certaine extension (.doc ou .xls par exemple) sont toujours exclus. Vous pouvez également ajouter d'autres extensions si vous ou votre entreprise souhaitez éviter d'envoyer certains fichiers.

La configuration de ThreatSense.Net est accessible depuis la fenêtre Configuration avancée, dans **Outils** > **ThreatSense.Net**. Sélectionnez l'option **Activer le système d'alerte anticipé ThreatSense** pour activer le système, puis cliquez sur le bouton **Configuration avancée...**.

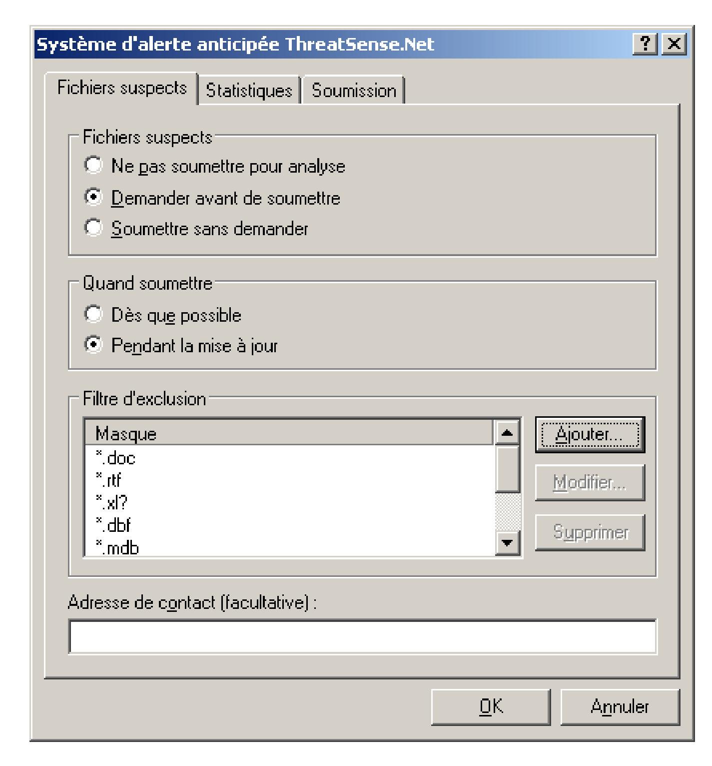


4.12.1 Fichiers suspects

L'onglet **Fichiers suspects** permet de configurer la manière dont les menaces sont soumises pour analyse au laboratoire de recherche sur les menaces d'ESET.

Si vous trouvez un fichier suspect, vous pouvez le soumettre à notre laboratoire de recherche sur les menaces pour analyse. S'il s'agit d'une application malveillante, sa détection est ajoutée à la prochaine mise à jour de la base des signatures de virus.

La soumission des fichiers peut être définie pour avoir lieu automatiquement. Vous pouvez également sélectionner l'option **Demander avant de soumettre** si vous souhaitez connaître les fichiers qui sont envoyés pour analyse et confirmer l'envoi.



Si vous ne souhaitez pas soumettre de fichiers, sélectionnez l'option **Ne pas soumettre pour analyse**. Le fait de choisir de ne pas soumettre les fichiers pour analyse n'a pas d'incidence sur la soumission des informations statistiques qui est configurée indépendamment (reportez-vous à la section Statistiques).

Quand soumettre : par défaut, l'option **Dès que possible** est sélectionnée pour que les fichiers suspects soient envoyés au laboratoire de recherche sur les menaces d'ESET. Ceci est recommandé lorsqu'une connexion Internet permanente est disponible et que les fichiers suspects peuvent être livrés très rapidement. Sélectionnez l'option **Pendant la mise à jour** pour que les fichiers suspects soient téléchargés vers ThreatSense.Net pendant la mise à jour suivante.

Filtre d'exclusion : cette option permet d'exclure certains fichiers/dossiers de la soumission. Par exemple, il peut être utile d'exclure des fichiers qui peuvent comporter des informations confidentielles, tels que des documents ou des feuilles de calcul. Les fichiers les plus ordinaires sont exclus par défaut (.doc, etc.). Vous pouvez ajouter des fichiers à la liste des fichiers exclus si vous le souhaitez.

Adresse de contact : votre **adresse de contact [facultative]** peut être envoyée avec les fichiers suspects et peut être utilisée pour vous contacter si des informations complémentaires sont nécessaires pour l'analyse. Notez que vous ne recevrez pas de réponse d'ESET, sauf si des informations complémentaires s'avèrent nécessaires.

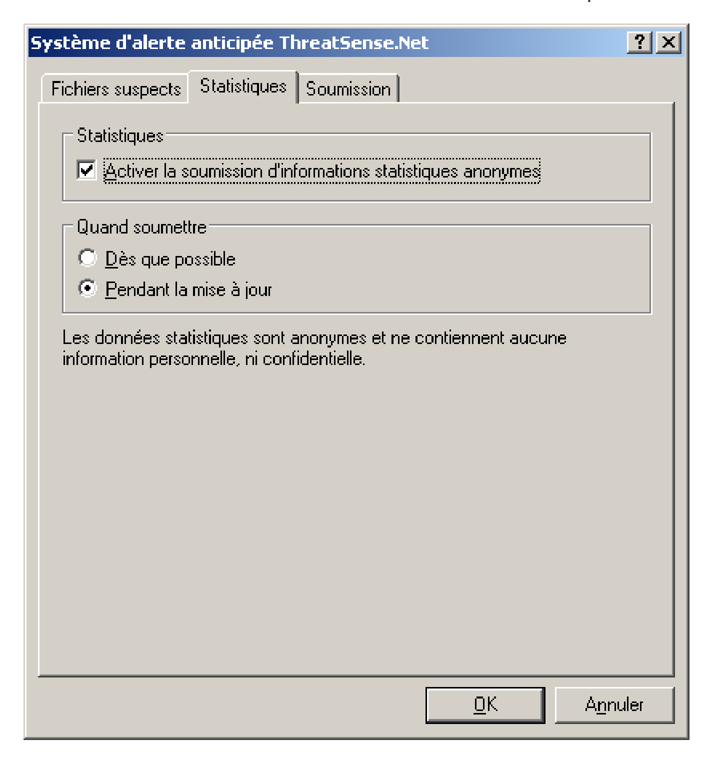
4.12.2 Statistiques

Le système d'alerte anticipé ThreatSense.Net collecte sur votre ordinateur des informations anonymes concernant les nouvelles menaces détectées. Ces informations peuvent inclure le nom de l'infiltration, la date et l'heure de détection, la version du produit de sécurité ESET, ainsi que des informations sur la version du système d'exploitation de votre ordinateur et ses paramètres régionaux. Les statistiques sont normalement fournies aux serveurs ESET une ou deux fois par jour.

Voici un exemple d'informations statistiques envoyées :

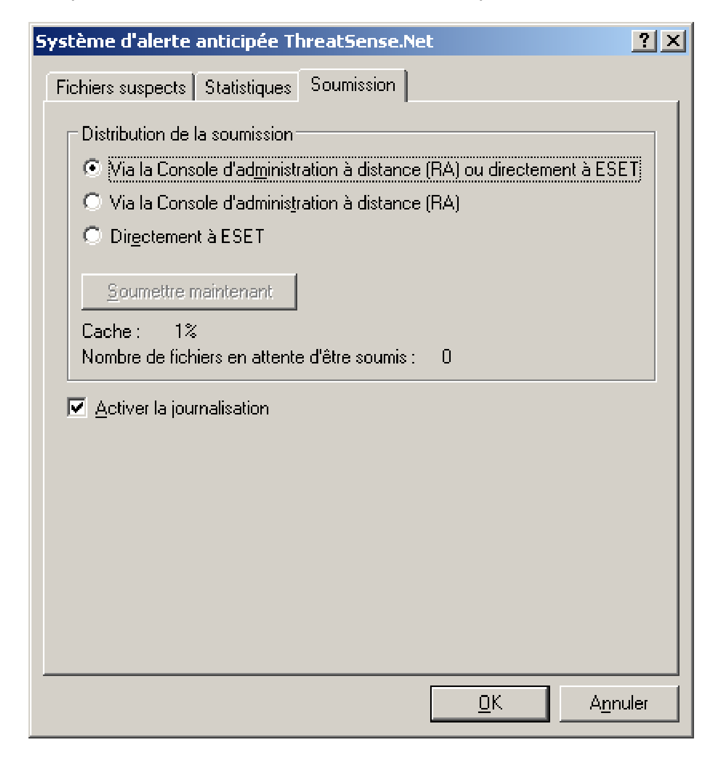
```
# utc_time=2005-04-14 07:21:28
# country="Slovaquie"
# language="ENGLISH"
# osver=5.1.2600 NT
# engine=5417
# components=2.50.2
# moduleid=0x4e4f4d41
# filesize=28368
# filename=C:\Documents and Settings\Administrator\Local Settings\Temporary Internet Files\Content.IE5\C14J8NS7\rdgFR1
```

Quand soumettre : vous pouvez définir le moment de l'envoi des informations statistiques. Si vous choisissez d'envoyer les informations statistiques **Dès que possible**, elles sont envoyées immédiatement après leur création. Ce choix convient si une connexion Internet est disponible en permanence. Si l'option **Pendant la mise à jour** est sélectionnée, toutes les informations statistiques sont envoyées collectivement pendant la mise à jour suivante.



4.12.3 Soumission

Vous pouvez sélectionner le mode d'envoi des fichiers et des informations statistiques à ESET. Sélectionnez l'option **Via la Console d'administration à distance (RA) ou directement à ESET** pour que les fichiers et les statistiques soient envoyés par tout moyen disponible. Sélectionnez l'option **Via la Console d'administration à distance (RA)** pour envoyer les fichiers et les statistiques au serveur d'administration à distance qui les envoie ensuite au laboratoire de recherche sur les menaces d'ESET. Si l'option **Directement à ESET** est sélectionnée, tous les fichiers suspects et les informations statistiques seront livrés directement par le programme au laboratoire d'ESET.



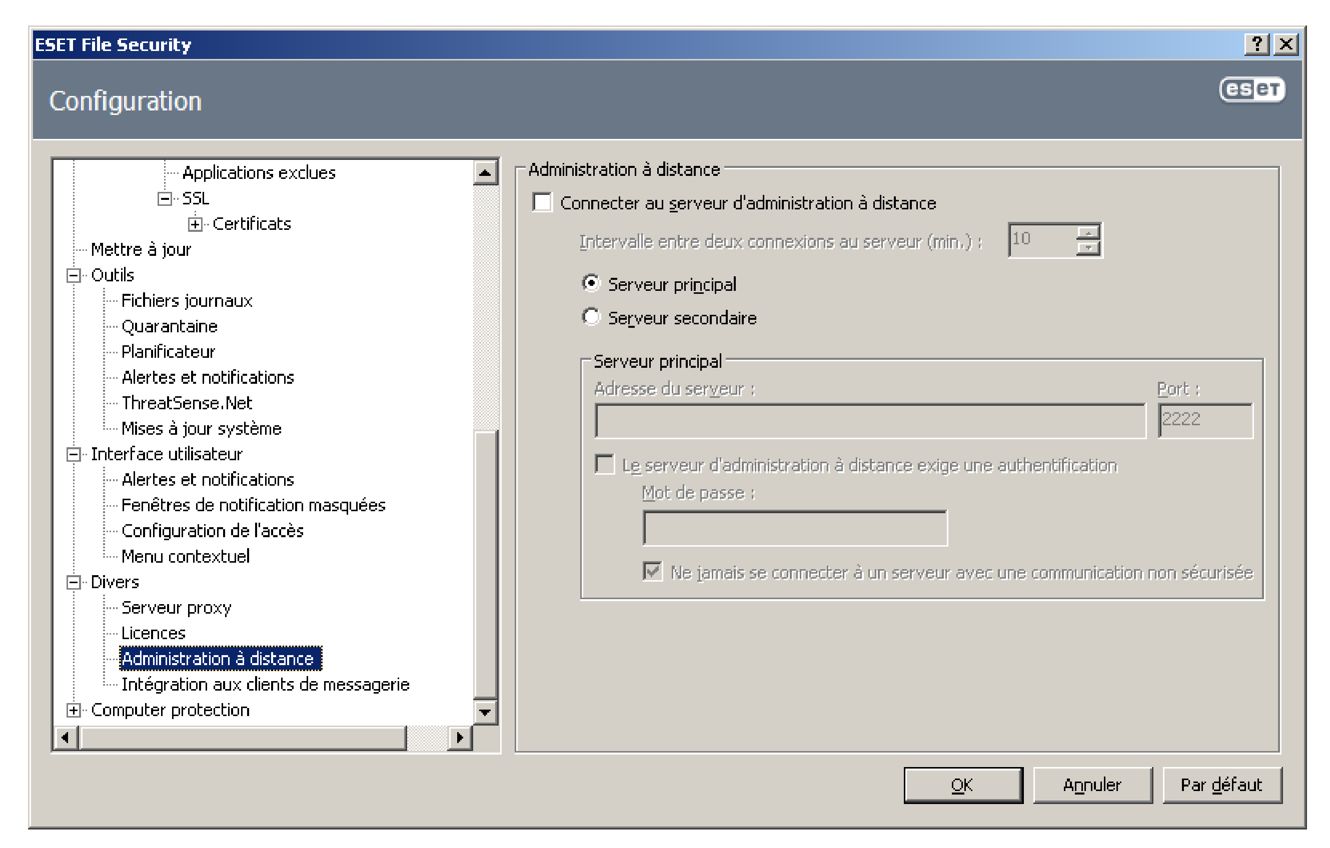
Si des fichiers sont en attente de soumission, le bouton **Soumettre maintenant** est activé. Cliquez sur ce bouton pour soumettre immédiatement les fichiers et les informations statistiques.

Activez l'option **Activer la journalisation** pour créer un journal permettant d'enregistrer les soumissions des fichiers et des informations statistiques.

4.13 Administration à distance

ESET Remote Administrator est un outil puissant permettant de gérer la stratégie de sécurité et qui offre une vision globale de la sécurité du réseau. Cet outil est particulièrement utile pour les grands réseaux. ESET Remote Administrator non seulement augmente le niveau de sécurité, mais permet également de gérer ESET File Security très facilement sur les postes de travail client.

Les options de configuration de l'administration à distance sont accessibles à partir de la fenêtre principale d'ESET File Security. Cliquez sur **Configuration** > **Accéder à la configuration avancée complète...** > **Divers** > **Administration à distance**.



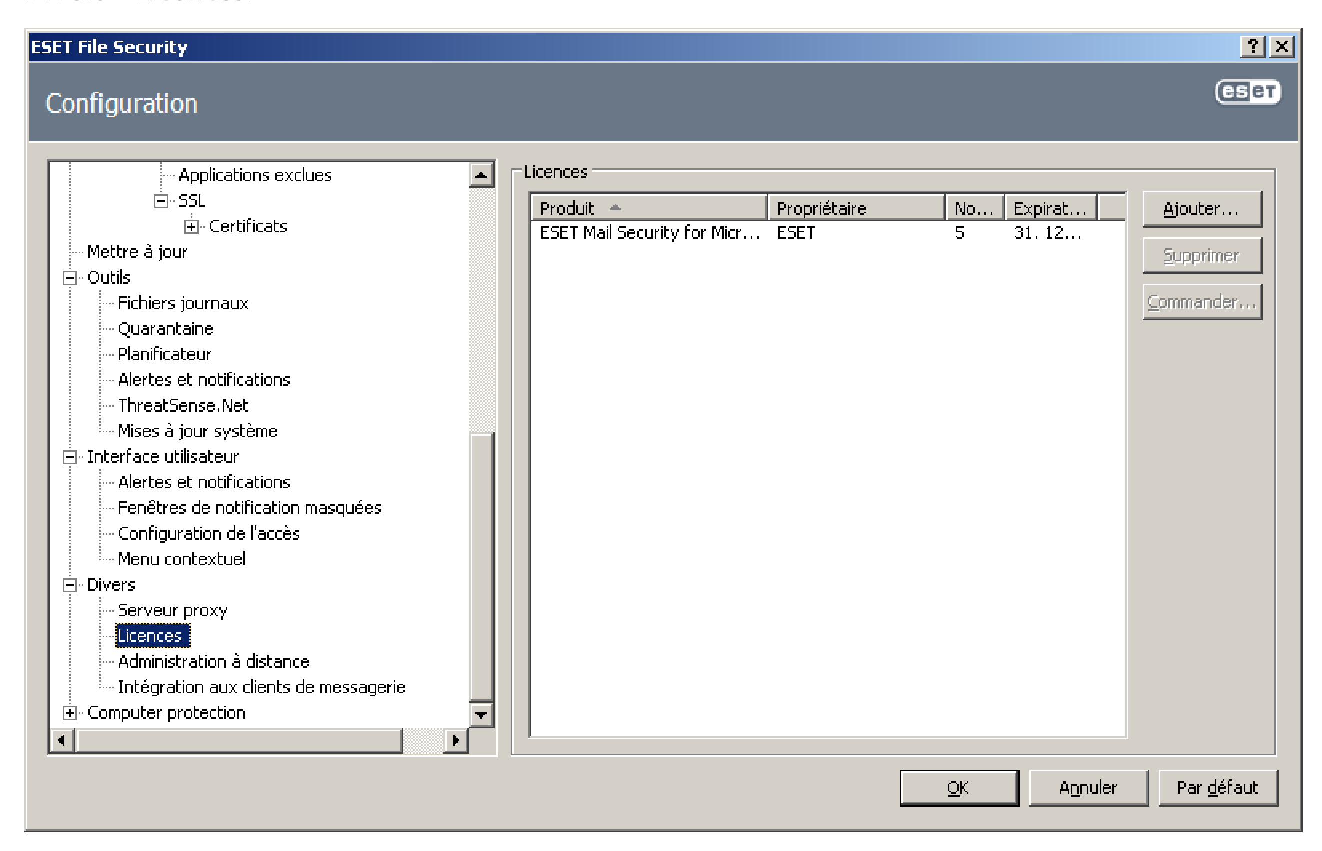
Activez l'administration à distance en sélectionnant l'option **Connecter au serveur d'administration à distance**. D'autres options sont également disponibles :

- **Intervalle entre deux connexions au serveur (min.) :** cette option indique la fréquence à laquelle ESET File Security se connecte à ESET Remote Administrator Server. Si la valeur est 0, les informations sont envoyées toutes les 5 secondes.
- **Adresse du serveur :** c'est l'adresse du serveur réseau où le serveur d'administration à distance est installé.
- **Port :** ce champ contient le port du serveur prédéfini utilisé pour la connexion. Il est recommandé de laisser le paramètre de port prédéfini sur 2222
- **Le serveur d'administration à distance exige une authentification :** Le serveur d'administration à distance exige une authentification.

Cliquez sur **OK** pour confirmer les modifications et appliquer les paramètres qu'utilise ESET File Security pour se connecter à ESET Remote Administrator Server.

4.14 Licences

La branche **Licences** vous permet de gérer les clés de licence d'ESET File Security et d'autres produits ESET tels que ESET Mail Security, etc. Après l'achat, les clés de licence sont fournies en même temps que le nom d'utilisateur et le mot de passe. Pour **ajouter/supprimer** une clé de licence, cliquez sur le bouton correspondant dans la fenêtre du gestionnaire de licences. Le gestionnaire de licences est accessible à partir de Configuration avancée complète sous **Divers** > **Licences**.



Une clé de licence est un fichier texte contenant des informations concernant le produit acheté : son propriétaire, le nombre de licences et la date d'expiration.

La fenêtre du gestionnaire de licences permet à l'utilisateur de charger et de voir le contenu de la clé de licence à l'aide du bouton **Ajouter...** ; les informations contenues sont affichées dans la fenêtre du gestionnaire. Pour supprimer des clés de licence de la liste, cliquez sur **Supprimer**.

Si une clé de licence est expirée et que vous êtes intéressé par le renouvellement de l'achat, cliquez sur le bouton **Commander...** : vous serez dirigé vers le site Web de la boutique en ligne.

5. Glossaire

5.1 Types d'infiltrations

Une infiltration est un élément de logiciel malveillant qui tente de s'introduire dans l'ordinateur d'un utilisateur et/ou de l'endommager.

5.1.1 Virus

Un virus est une infiltration qui endommage les fichiers existants de votre ordinateur. Les virus informatiques sont comparables aux virus biologiques parce qu'ils utilisent des techniques similaires pour se propager d'un ordinateur à l'autre.

Les virus informatiques attaquent principalement les fichiers et documents exécutables. Pour proliférer, un virus attache son « corps » à la fin d'un fichier cible. En bref, un virus informatique fonctionne de la manière suivante : après l'exécution du fichier infecté, le virus s'active lui-même (avant l'application originale) et exécute sa tâche prédéfinie. C'est après seulement que l'application originale peut s'exécuter. Un virus ne peut pas infecter un ordinateur à moins qu'un utilisateur n'exécute ou n'ouvre lui-même (accidentellement ou délibérément) le programme malveillant.

Les virus peuvent varier en fonction de leur gravité et de leur cible. Certains sont extrêmement dangereux parce qu'ils ont la capacité de supprimer délibérément des fichiers du disque dur. D'autres, en revanche, ne causent pas de réels dommages : ils ne servent qu'à gêner l'utilisateur et à démontrer les compétences techniques de leurs auteurs.

Il est important de noter que, contrairement aux chevaux de Troie et aux logiciels espions, les virus sont de plus en plus rares, car d'un point de vue commercial, ils ne sont pas très attrayants pour les auteurs de programmes malveillants. En outre, le terme « virus » est souvent utilisé mal à propos pour couvrir tout type d'infiltrations. On tend à le remplacer progressivement par le terme « logiciel malveillant » ou « malware » en anglais.

Si votre ordinateur est infecté par un virus, il est nécessaire de restaurer les fichiers infectés à leur état original, c'est-à-dire de les nettoyer à l'aide d'un programme antivirus.

Dans la catégorie des virus, on peut citer : OneHalf, Tenga et Yankee Doodle.

5.1.2 Vers

Un ver est un programme contenant un code malveillant qui attaque les ordinateurs hôtes et se propage via un réseau. La différence fondamentale entre les virus et les vers réside dans le fait que les vers ont la capacité de se répliquer et de voyager par eux-mêmes. Ils ne dépendent pas des fichiers hôtes (ou des secteurs d'amorçage). Les vers se propagent par l'intermédiaire d'adresses de messagerie de votre liste de contacts ou exploitent les vulnérabilités de sécurité des applications réseau.

Les vers sont ainsi susceptibles de vivre beaucoup plus longtemps que les virus. Par le biais d'Internet, ils peuvent se propager à travers le monde en quelques heures seulement et parfois en quelques minutes. Leur capacité à se répliquer indépendamment et rapidement les rend plus dangereux que les autres types de programmes malveillants.

Un ver activé dans un système peut être à l'origine de plusieurs dérèglements : il peut supprimer des fichiers, dégrader les performances du système ou même désactiver certains programmes. Par nature, il peut servir de « moyen de transport » à d'autres types d'infiltrations.

Si votre ordinateur est infecté par un ver, il est recommandé de supprimer les fichiers infectés, car ils contiennent probablement du code malveillant.

Parmi les vers les plus connus, on peut citer : Lovsan/Blaster, Stration/Warezov, Bagle et Netsky.

5.1.3 Chevaux de Troie

Dans le passé, les chevaux de Troie étaient définis comme une catégorie d'infiltrations dont la particularité est de se présenter comme des programmes utiles pour duper ensuite les utilisateurs qui acceptent de les exécuter. Il est cependant important de remarquer que cette définition s'applique aux anciens chevaux de Troie. Aujourd'hui, il ne leur est plus utile de se déguiser. Leur unique objectif est de trouver la manière la plus facile de s'infiltrer pour accomplir leurs desseins malveillants. Le terme « cheval de Troie » est donc devenu un terme très général qui décrit toute infiltration qui n'entre pas dans une catégorie spécifique.

La catégorie étant très vaste, elle est souvent divisée en plusieurs sous-catégories :

- **Téléchargeur** : programme malveillant qui est en mesure de télécharger d'autres infiltrations sur Internet.
- **Dropper** : type de cheval de Troie conçu pour déposer d'autres types de logiciels malveillants sur des ordinateurs infectés.
- **Backdoor** : application qui communique à distance avec les pirates et leur permet d'accéder à un système et d'en prendre le contrôle.
- **Keylogger** (keystroke logger) : programme qui enregistre chaque touche sur laquelle tape l'utilisateur avant d'envoyer les informations aux pirates.
- **Composeur** : programme destiné à se connecter à des numéros surtaxés. Il est presque impossible qu'un utilisateur remarque la création d'une nouvelle connexion. Les composeurs ne peuvent porter préjudice qu'aux utilisateurs ayant des modems par ligne commutée, qui sont de moins en moins utilisés.

Les chevaux de Troie prennent généralement la forme de fichiers exécutables avec l'extension .exe. Si un fichier est identifié comme cheval de Troie sur votre ordinateur, il est recommandé de le supprimer, car il contient sans doute du code malveillant.

Parmi les chevaux de Troie les plus connus, on peut citer : NetBus, Trojandownloader. Small.ZL, Slapper

5.1.4 Rootkits

Les rootkits sont des programmes malveillants qui procurent aux pirates un accès illimité à un système tout en dissimulant leur présence. Après avoir accédé au système (généralement en exploitant une faille), les rootkits utilisent des fonctions du système d'exploitation pour se protéger des logiciels antivirus : ils dissimulent des processus, des fichiers et des données de la base de registre Windows. Pour cette raison, il est presque impossible de les détecter à l'aide des techniques de test ordinaires.

Il existe deux niveaux de détection permettant d'éviter les rootkits :

1) Lorsqu'ils essaient d'accéder au système. Ils ne sont pas encore installés et donc inactifs. La plupart des antivirus sont en mesure d'éliminer les rootkits à ce niveau (en supposant qu'ils détectent effectivement les fichiers comme infectés).

2) Lorsqu'ils sont inaccessibles aux tests habituels. Les utilisateurs ESET File Security bénéficient de la technologie Anti-Stealth qui permet de détecter et d'éliminer les rootkits en activité.

5.1.5 Logiciels publicitaires

Le terme anglais « adware » désigne les logiciels soutenus par la publicité. Les programmes qui affichent des publicités entrent donc dans cette catégorie. Les logiciels publicitaires ouvrent généralement une nouvelle fenêtre contextuelle automatiquement dans un navigateur Internet. Cette fenêtre contient de la publicité ou modifie la page de démarrage du navigateur. Ils sont généralement associés à des programmes gratuits et permettent aux développeurs de couvrir les frais de développement de leurs applications (souvent utiles).

Les logiciels publicitaires en tant que tels ne sont pas dangereux ; ils dérangent simplement les utilisateurs en affichant des publicités. Le danger réside dans le fait qu'ils peuvent également avoir des fonctions d'espionnage (comme les logiciels espions).

Si vous décidez d'utiliser un logiciel gratuit, soyez particulièrement attentif au programme d'installation. La plupart des programmes d'installation vous avertissent en effet qu'ils installent également un programme publicitaire. Dans la plupart des cas, vous pourrez désactiver cette installation supplémentaire et installer le programme sans logiciel publicitaire.

Certains programmes refusent de s'installer sans leur logiciel publicitaire ou voient leurs fonctionnalités limitées. Cela signifie que les logiciels publicitaires accèdent souvent au système de manière « légale », dans la mesure où les utilisateurs l'ont accepté. Dans ce cas, il est préférable de procéder avec prudence. Si un logiciel publicitaire est détecté sur votre ordinateur, il est conseillé de le supprimer, car il est fort probable qu'il contienne du code malveillant.

5.1.6 Logiciels espions

Cette catégorie englobe toutes les applications qui envoient des informations confidentielles sans le consentement des utilisateurs et à leur insu. Les logiciels espions utilisent des fonctions de traçage pour envoyer diverses données statistiques telles que la liste des sites Web visités, les adresses e-mail de la liste de contacts de l'utilisateur ou la liste des touches du clavier utilisées.

Les auteurs de ces logiciels espions affirment que ces techniques ont pour but d'en savoir plus sur les besoins et intérêts des utilisateurs afin de mieux cibler les offres publicitaires. Le problème est qu'il n'y a pas de distinction claire entre les applications utiles et les applications malveillantes, et que personne ne peut garantir que les informations récupérées ne sont pas utilisées à des fins frauduleuses. Les données récupérées par les logiciels espions peuvent être des codes de sécurité, des codes secrets, des numéros de compte bancaire, etc. Les logiciels espions sont souvent intégrés aux versions gratuites d'un programme dans le but de générer des gains ou d'inciter à l'achat du logiciel. Les utilisateurs sont souvent informés de la présence d'un logiciel espion au cours de l'installation d'un programme qui vise à les inciter à acquérir la version payante qui en est dépourvue.

Parmi les produits logiciels gratuits bien connus qui contiennent des logiciels espions, on trouve les applications clients de réseaux P2P (poste à poste). Spyfalcon ou Spy Sheriff (et beaucoup d'autres) appartiennent à une sous-catégorie spécifique de logiciels espions : ils semblent être des programmes antispyware alors qu'ils sont en réalité eux-mêmes des logiciels espions.

Si un fichier est détecté comme logiciel espion sur votre ordinateur, il est préférable de le supprimer, car il est fort probable qu'il contienne du code malveillant.

5.1.7 Applications potentiellement dangereuses

Il existe de nombreux programmes authentiques qui permettent de simplifier l'administration des ordinateurs en réseau. Toutefois, s'ils tombent entre de mauvaises mains, ces programmes sont susceptibles d'être utilisés à des fins malveillantes. ESET File Security permet de détecter ces menaces.

Les applications potentiellement dangereuses rentrent dans une classification utilisée pour les logiciels commerciaux légitimes. Cette classification comprend les programmes d'accès à distance, les applications de résolution de mot de passe ou les keyloggers (programmes qui enregistrent chaque frappe au clavier de l'utilisateur).

Si vous découvrez qu'une application potentiellement dangereuse est présente et fonctionne sur votre ordinateur (sans que vous l'ayez installée), consultez l'administrateur réseau ou supprimez l'application.

5.1.8 Applications potentiellement indésirables

Les applications potentiellement indésirables ne sont pas nécessairement malveillantes, mais elles sont susceptibles d'affecter les performances de votre ordinateur. Ces applications sont habituellement installées après consentement. Si elles sont présentes sur votre ordinateur, votre système se comporte différemment (par rapport à son état avant l'installation). Voici les changements les plus significatifs :

- affichage de nouvelles fenêtres ;
- activation et exécution de processus cachés ;
- utilisation plus importante des ressources système ;
- modification des résultats de recherche ;
- communication de l'application avec des serveurs distants.